Vysoká škola báňská – Technická univerzita Ostrava

Ekonomická fakulta

KATEDRA SYSTÉMOVÉHO INŽENÝRSTVÍ

Průzkum stavu zajištění organizační a technické bezpečnosti IT na VŠ

Survey on the Current State of Securing Organizational and Technical Security of IT at Universities

Student: Břetislav Glac

Vedoucí diplomové práce: doc. Ing. Milena Tvrdíková, CSc.

Ostrava 2015

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra aplikované informatiky

Zadání diplomové práce

Student: **Bc. Břetislav Glac**

Studijní program: N6209 Systémové inženýrství a informatika

Studijní obor: 6209T025 Systémové inženýrství a informatika

Téma: Průzkum stavu zajištění organizační a technické bezpečnosti IT na VŠ
Survey on the Current State of Securing Organizational and Technical Security of IT at Universities

Zásady pro vypracování:

1. Úvod
2. Nové trendy v IT a jejich vliv na bezpečnost na VŠ
3. Analýza současného stavu informační bezpečnosti na VŠ
4. Vyhodnocení průzkumu
5. Návrh doporučení pro zvýšení bezpečnosti na VŠ
6. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

DOUCEK, Petr a kol. *Řízení bezpečnosti informací.* 2. vyd. Praha: Professional Publishing, 2011. 286. s. ISBN 978-80-7431-050-8.
ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. 3777 s. ISBN 978-80-7204-872-4.
RHODES-OUSLEY, Mark. *Information Security: the Complete Reference.* 2nd ed. New York: McGraw Hill, 2012. 896 p. ISBN 978-007-1784-351.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **doc. Ing. Milena Tvrdíková, CSc.**

Datum zadání: 21.11.2014
Datum odevzdání: 25.04.2015

Ing. Petr Rozehnal, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Místopřísežné prohlášení

Místopřísežně prohlašuji, že jsem celou bakalářskou práci vypracoval samostatně a všechny použité zdroje uvádím v seznamu použité literatury. Příloha č. 1 daná mi k dispozici, jsem samostatně doplnil.

V Ostravě dne 15.7.2015 Podpis: ……

Břetislav Glac

OBSAH

1 Úvod

Informace je důležitým zdrojem, podle kterého lze řídit a podle kterého je možné se rozhodovat. Také je nutné informace chránit před nebezpečnými vlivy, ale se stále rychlejším rozvojem technologií, se obor informační bezpečnosti neustále mění a je třeba na to brát ohled. Technologický rozvoj v této oblasti přináší nové hrozby, jimž je nutné se věnovat a zaměřit se na ně, ale také nové výzvy, kterým je třeba čelit.

Mezi technologie, které se velmi rychle mění, vylepšují a těší se stále větší oblibě, patří ty mobilní a těm bude věnována první kapitola. Chytré telefony, tablety a phablety jsou neskutečně výkonná zařízení, která se lehce vyrovnají výkonem třeba s notebooky vyrobenými před pár lety. Výkon, který se vejde do tak malého zařízení je neuvěřitelný, a vytváří tak prostor, aby se z nich stali nedocenitelní pomocníci do každodenního života, a to jak pracovního, tak osobního. A tyto přednosti jsou zároveň zdrojem vážných hrozeb, ale nejen ty. Nejenže se stále zvyšuje výpočetní výkon, ale zároveň vývoj samotných operačních systémů velmi mění celé prostředí, na které musí informační bezpečnost reagovat. A právě cílem této kapitoly je identifikovat hrozby související s používáním mobilních technologií, popsat možnosti, jak je možné se s nimi vypořádat a nastínit také to, jaký vliv tohle vše může mít v univerzitním a vysokoškolském prostředí.

Netřeba zdůrazňovat, že moderní mobilní technologie ve svých pamětech obsahují nespočet informací a to nejen osobních, ale i firemních. Těmi mohou být různé kontaktní informace, záznamy komunikace, historie polohy zařízení, fotografie a mnoho dalšího. A tady už se jedná o informace, které je nutné chránit nejen před zneužitím, ale i jejich zničením.

Hlavním cílem diplomové práce pak je analýza organizační a technické bezpečnosti, jinými slovy v podstatě informační bezpečnosti, na vysokých školách. Tomuto tématu se věnují zbývající kapitoly. Tato analýza bezpečnosti pak bude výchozím bodem pro další vyhodnocení získaných informací, popsání současného stavu zabezpečení a podkladem pro návrh případných zlepšení bezpečnostních opatření.

2 NOVÉ TRENDY V IT A JEJICH VLIV NA BEZPEČNOST NA VŠ

Digitální revoluce a stálý pokrok ve vývoji informačních technologií přináší do firemní a potažmo i univerzitní sféry stále nové možnosti jejich využití. Důvody jsou zřejmé, ulehčení práce, usnadnění přístupu k datům a informacím či finanční úspory. Mezi dnes asi nejrychleji se rozvíjející patří mobilní technologie, zejména stále více používané tzv. smartphony (chytré telefony) a tablety. Nicméně přes veškeré výhody, které se s jejich využitím a používáním pojí, s sebou přinášejí i mnohá bezpečnostní rizika. Také analogie mezi firemním a univerzitním prostředím je na místě. Stejně jako firmy, tak i univerzity mají své zaměstnance a své zákazníky, kterými jsou studenti. A to je také důvodem, proč lze na tyto subjekty z hlediska bezpečnosti informací nahlížet velmi podobně.

V této kapitole tedy budou popsána rizika, která vyplývají z používání moderních technologií, ale ještě před tím je nutné vymezit, co to informační bezpečnost v rámci organizace je a jaké pojmy se v souvislosti s ní používají (Matoušková, 2013).

2.1 Informační bezpečnost

Každá organizace disponuje určitým množstvím informací a právě informace patří mezi velmi ceněná aktiva vytvářející hodnotu, proto je nutné je chránit. Informační bezpečnost, respektive bezpečnost informací (Information Security) je podle Doucka (2011, s. 55) „*ochrana důvěrnosti, integrity a dostupnosti informací. Kromě toho může také zahrnovat další vlastnosti, například autenticitu, odpovědnost, nepopiratelnost a spolehlivost.“* Cílem je zabezpečit informace již od jejich vzniku pomocí množství opatření zajišťujících uchování výše zmíněných atributů.

Ve spojitosti s informační bezpečností je třeba zmínit se o dalších dvou pojmech, o bezpečnosti organizace a bezpečnosti IS/ICT. Vztah, který mezi nimi existuje, je znázorněn na obr. 2-1 Na nejvyšším stupni je bezpečnost organizace, jejímž úkolem je zajištění objektů organizace a tedy veškerého majetku. Právě její součástí je mimo jiné i bezpečnost informací. Z postavení informační bezpečnosti ve středu je možno vydedukovat, že jejím cílem není sdružovat zásady o ochraně informací pouze v digitální podobě. Zahrnuje bezpečnou práci se všemi druhy informací, například způsob jejich zpracování, archivace v digitální i nedigitální podobě, přenos či skartace. Samotná bezpečnost IS/ICT se zabývá ochranou pouze těch aktiv,

které jsou součástí informačních systému v rámci informačních a komunikačních technologií dané organizace (Ondrák, 2013).

Obr. 2-1: Vzájemné vztahy bezpečností v organizaci

Zdroj: (Ondrák, 2013, s. 14)

2.1.1 Základní pojmy v souvislosti s informační bezpečností

Již ze samotné definice informační bezpečnosti vzešlo několik pojmů, které je nutno blíže vysvětlit, aby nedošlo k jejich nesprávné interpretaci.

Aktiva jsou veškeré hmotné i nehmotné statky, tedy to, co pro organizaci má nějakou hodnotu. Mezi hmotná aktiva se řadí například technické prostředky (hardware, kabelové rozvody, komunikační technologie a další technické prostředky) či budovy a mezi nehmotná pak software (programové vybavení, operační systémy ad.), pracovní postupy a v neposlední řadě i data a informace, jež se řadí mezi nejcennější aktiva organizace.

Důvěrnost je zajištění toho, že informace je poskytnuta pouze těm, kteří mají autorizaci k jejímu zobrazení či použití. Obecně je toto možné interpretovat tak, že jeden soubor dat je přístupný autorizovaným osobám nebo systémům, přičemž nikdo jiný se k těmto datům nesmí dostat (Rhodes-Ousley, 2012).

Integrita se vztahuje k zabezpečení informací proti jejich změně neautorizovaným způsobem. Je nezbytné postarat se o to, aby informace byla úplná a správná.

Dostupnost v kontextu informační bezpečnosti znamená, že informace je přístupná a použitelná na žádost autorizované entity a v době, kdy je potřebná.

Hrozba je možná událost, jejímž následkem může nastat poškození systému nebo organizace. Jedná se o zneužití zranitelnosti. Hrozby mohou být různého charakteru. Rozlišují se přírodní a fyzické (živelné katastrofy, požáry, přerušení dodávky elektrického proudu atd.), technické a technologické (poškození nosičů dat, poruchy způsobené nesprávně fungujícími programy, závady komponent IS/ICT apod.) a lidské. Hrozby lidského charakteru se ještě dále dělí na neúmyslné (způsobené neznalostí nebo nedbalostí) a úmyslné, jejichž působení může přicházet zvenčí anebo zevnitř organizace (Doucek, 2011).

Zranitelnost je slabé místo aktiva nebo opatření, které může vézt k tomu, aby se hrozba z potenciální stala reálnou, a tím tedy způsobila škodu. Zranitelnost je vlastností aktiva, přičemž každé aktivum je zranitelné, jelikož jeho hodnota je ohrožována různými vlivy (Rhodes-Ousley, 2012).

Dopad je následek působení hrozby, jinými slovy je to škoda způsobená incidentem. Dopady mohou být různé povahy, od těch, které jsou ve výsledku zřetelné a jejich účinek lze ihned pozorovat a mnohdy i jednoduše vyčíslit (např. zničení nebo poškození aktiva) až po ty, jejichž následky se nedostaví ihned, ale je možné je pozorovat postupně (poškození image organizace, periodický únik informací apod.). V rámci možností je vhodné dopady hrozeb vyčíslit peněžně, a to z důvodu porovnání s náklady na opatření (Doucek, 2011).

Opatření je dle normy ISO/IEC 27000:2014 (2014, s. 2) prostředek pro úpravu či modifikaci rizika. Opatření zahrnuje jakýkoliv proces, politiku, zařízení, postup či libovolnou činnost, která riziko ovlivňuje, přičemž ne vždy musí být výsledkem požadovaný nebo očekávaný účinek. Opatření se rozdělují podle charakteru na:

- administrativní – mezi tato opatření jsou řazeny hlavně různé směrnice pro práci s IS/ICT v organizaci,
- fyzická – zde patří např. používání identifikačních karet do prostor s omezeným přístupem,
- technická a technologická – mezi ně patří např. autorizace a autentizace uživatelů nebo bezpečnostní politiky ohledně hesel.

Primárním cílem opatření je tedy celkově zmírnit možnost hrozby, případně jejího dopadu, ale i cíle lze rozčlenit do několika skupin:

- prevenční – minimalizování hrozeb ještě předtím, než k nim dojde; často se využívá automatizovaných postupů, které eliminují selhání nejen lidského faktoru (automatické zámky bezpečnostních dveří, odhlášení ze systému při nečinnosti apod.),
- detekční – vyhledávání potenciálních nežádoucích událostí např. využitím monitorovacích systémů,
- korekční – zmírnění dopadu a minimalizace škod v době, kdy již jsou znát následky uskutečněné hrozby; např. obnova dat z poškozených záznamových medií (Doucek, 2011).

Riziko je pravděpodobnost, že působením dané hrozby dojde ke zničení nebo poškození hodnoty aktiva. Jak je uvedeno v normě ISO/IEC 27000:2014 (2014, s. 8-9) riziko je často vyjádřeno jako kombinace dopadu hrozby a s ní související pravděpodobností výskytu. Riziko informační bezpečnosti je spojováno s možností, že hrozba využije zranitelnosti informačního aktiva nebo skupiny informačních aktiv a tím poškodí organizaci.

Zbytkové riziko je definováno jako to, co zůstane po aplikování opatření. Většinou totiž nelze rizika úplně odstranit, ale pouze zmírnit, a je tedy nutné zvážit, zda je již toto riziko akceptovatelné (Rhodes-Ousley, 2012).

2.2 Moderní mobilní technologie

Moderní mobilní zařízení, smartphony neboli chytré telefony, jsou zařízení, která v sobě kombinují prvky klasických mobilních telefonů a osobních počítačů. Z mobilních telefonů převzaly základní funkce telefonování a posílání textových zpráv, z počítačů zase poměrně výkonný hardware. Z hlediska informační bezpečnosti jsou však podstatné funkce a vlastnosti, které tyto zařízení činí nedocenitelnými pomocníky v každodenním životě. Řeč je zejména o pokročilém operačním systému, kterým disponují, a v drtivé většině jejich možnosti připojit se k internetu prostřednictvím mobilních sítí operátorů a bezdrátovým počítačovým sítím. Dalším typem moderního mobilního zařízení je tablet, který se od smartphonu odlišuje tím, že jeho uživateli prostřednictvím mobilního operátora neposkytuje hlasové služby a možnost posílání textových zpráv, ale stále je v některých případech výrobci

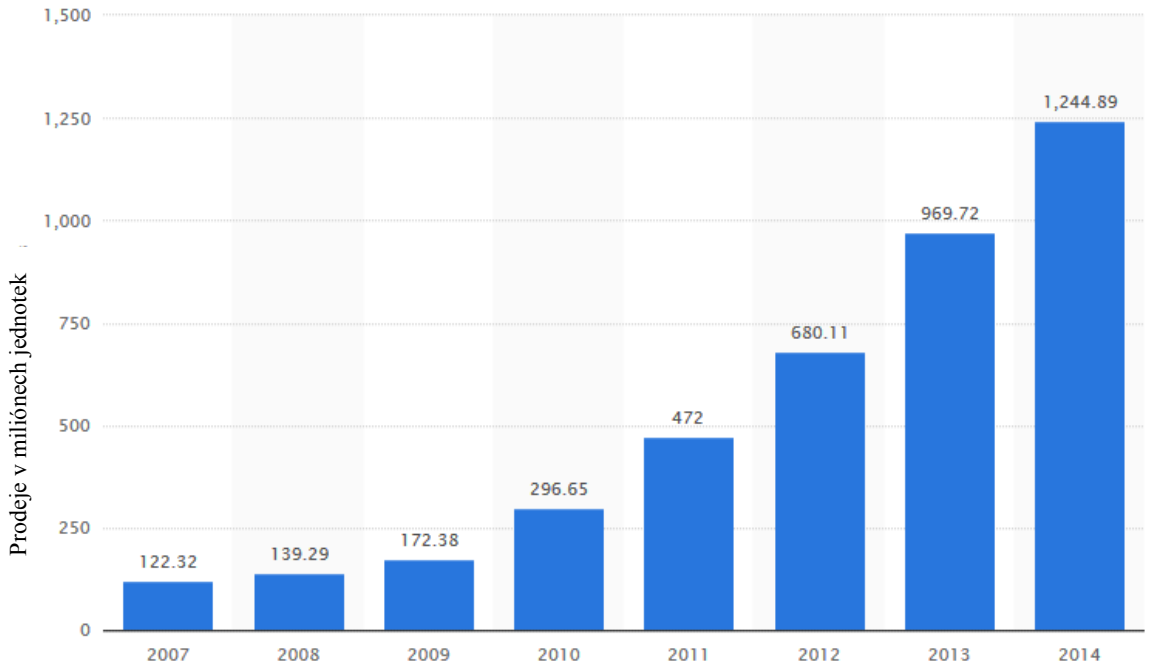
vybavili možností připojit se k mobilním datovým sítím. Na druhou stranu v mnoha případech disponují výkonnějším hardwarem a zejména větším displejem. Do rodiny těchto zařízení ještě patří phablet, zařízení v sobě kombinující vetší velikost displeje a výkonnější hardware tabletů a možnost využívání hlasových služeb telefonů. Název zařízení je kombinací slov phone (telefon) a tablet.

Americký Národní institut standardů a technologie (NIST SP 800-124, 2013, s. 2) definuje mobilní zařízení na základě jeho hardwarových a softwarových charakteristik jako:

- zařízení malých rozměrů,
- zařízení s alespoň jedním bezdrátovým síťovým rozhraním pro přístup do sítě Internet; toto rozhraní může využívat Wi-Fi, mobilní sítě nebo jinou technologii umožňující připojit zařízení do síťové infrastruktury, která disponuje konektivitou k Internetu,
- zařízení s lokálním, vestavěným a nevyjímatelným datovým úložištěm,
- zařízení s operačním systémem, který není plnohodnotným desktopovým nebo laptopovým operačním systémem, jinými slovy s mobilním operačním systémem, mezi které se řadí např. Android, Windows Phone, iOS, BlackBerry OS, Symbian ad.,
- zařízení, pro které jsou aplikace dostupné více metodami (poskytované s operačním systémem, přístupné pomocí webového prohlížeče anebo získané a nainstalované od třetích stran),
- zařízení s vestavěnými funkcemi pro synchronizaci lokálních dat se vzdálenými umístěními (jinými počítači, servery organizací, servery poskytovatelů telekomunikačních služeb, jinými servery třetích stran atd.).

V posledních letech je možno pozorovat rapidní nárůst uživatelů smartphonů nejen mezi běžnou populací, ale tyto zařízení se také velmi rychle prosazují i uvnitř organizací. Trend s jakou rychlostí se smartphony dostávají mezi koncové uživatele je možno pozorovat na obr. 2-2. Proč se mobilní zařízení v organizacích tak rychle adaptují má hned několik prostých důvodů. Velikost zařízení umožňuje mít jej stále po ruce, vysoká konektivita poskytuje uživateli možnost připojit se k vnitřní síti organizace téměř odkudkoliv a výkonný hardware zajišťuje množství funkcí, které uživatel může využít podobně, jako když pracuje na notebooku nebo osobním počítači. Takovými funkcemi mohou být např. plánování schůzek, přístup k emailové schránce, synchronizace a sdílení pracovního kalendáře, pořádání online

schůzek se spolupracovníky, dostupnost pracovních dat a informací téměř odkudkoliv ad. Všechny tyto možnosti mohou vést k neuvěřitelnému nárůstu efektivity a produktivity práce. Stačí si představit to, že člověk při cestě do práce hromadnou dopravou nemusí jen sedět a čekat na příjezd, ale během cesty může vyřídit pracovní korespondenci, zkontrolovat kalendář a tím efektivně využít svůj čas.



Obr. 2-2: Počet smartphonů prodaných koncovým uživatelům mezi roky 2007-2014
Zdroj: [http://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/]

Avšak tyto nepřeberné možnosti, jak mobilní zařízení využívat, s sebou přinášejí i mnohé bezpečnostní hrozby, které budou popsány dále.

2.2.1 Hrozby spojené s používáním mobilních technologií uvnitř vysokoškolské sítě a jejich možné dopady

Jak již bylo popsáno v předcházející kapitole, tak z charakteristiky mobilního zařízení vyplývá množství bezpečnostních hrozeb, které mohou mít nemalý vliv na bezpečnost vnitřní sítě a na IS/ICT provozované v rámci této sítě. Avšak v rámci vysokoškolské počítačové sítě je nutné na mobilní zařízení nahlížet z několika různých perspektiv, a to z perspektivy uživatelské, kdy zařízení mohou obsluhovat studenti nebo zaměstnanci, a vlastnické, kdy mobilní zařízení je či není majetkem univerzity. V případě uživatelského hlediska hrozby vyplývající ze studentských mobilních zařízení budou působit odlišným způsobem a budou mít i rozdílné dopady oproti mobilním zařízením zaměstnanců univerzit. Důvodem je, že

zaměstnanci mají autorizovaný přístup k většímu množství dat a přístup do většího počtu systémů. V tomto ohledu je také nutné brát v úvahu počty těchto zařízení, jelikož je nezbytné počítat s větším množstvím studentů oproti zaměstnancům.

Dále budou popsány hrozby, které se přímo týkají a jsou typické pro mobilní zařízení, případně jejich používáním se riziko zvyšuje. Samotná bezpečnostní opatření vztažená k těmto hrozbám budou předmětem jedné z dalších kapitol.

a) Hrozba ztráty nebo odcizení mobilního zařízení

Jak již bylo zmíněno výše, tak mobilní zařízení dosahují malých rozměrů. Z toho vyplývá bezesporu mnoho výhod, jako je jejich používání prakticky kdekoliv. Avšak jejich velikost je současně nevýhodou, jelikož zvyšuje pravděpodobnost ztráty či odcizení oproti jiným zařízením (např. notebooky, které jsou několikanásobně větší a těžší, tudíž všimnout si, že chybí, je snazší) a v důsledku toho mohou být ohrožena citlivá data uložená v zařízení nebo v externí paměti.

V případě studentských zařízení, přestože jejich počty jsou větší, nemusí být dopad tak velký, protože se v ohrožení ocitnou zejména osobní data a ne citlivá data univerzit. Na druhou stranu zaměstnanecká zařízení představují mnohem větší hrozbu. Ta mohou obsahovat interní elektronickou poštu nebo důležité dokumenty obsahující citlivá data, jež představují mnohem větší riziko zneužití útočníkem. Velkým problémem pak mohou být přihlašovací údaje uložené v paměti zařízení, případně v internetových prohlížečích, což riziko zneužití v konečném důsledku ještě více zvyšuje a útočník takovým způsobem může získat přístup k různým systémům. Další pesimistický scénář pak je ten, kdy mobilní zařízení je jediným místem, kde se nachází data organizace, a jeho ztráta nebo zcizení pak znamená i ztrátu dat.

V roce 2012 provedla společnost Symantec průzkum v pěti amerických městech, co se stane se ztraceným smartphonem. V každém z těchto měst bylo úmyslně „ztraceno“ 50 mobilních zařízení, ve kterých se nacházela simulovaná osobní a firemní data. Telefony umožňovaly vzdáleně monitorovat, co se s nimi stane po nalezení. Bylo zjištěno, že v 83 % případů se nálezce pokusil o přístup k firemním datům a ve 45 % případů byl zjištěn pokus o přístup k firemní emailové schránce. Ve smartphonu byly uloženy 2 soubory, soubor „HR Salaries“ (informace o mzdách), který byl zobrazen v 53 % případů, a soubor „HR Cases“ byl zobrazen na 40 % zařízení. Původního majitele zařízení se nakonec pokusila

vyhledat polovina nálezců. Tato zjištění demonstrují, jak velkým rizikem mohou být mobilní zařízení v případě jejich ztráty. Symantec také zkoumal co se děje s osobními daty v zařízení, ale ta nejsou pro tuto práci podstatná (Symantec, ©2012).

b) Hrozba neúmyslného zpřístupnění citlivých dat

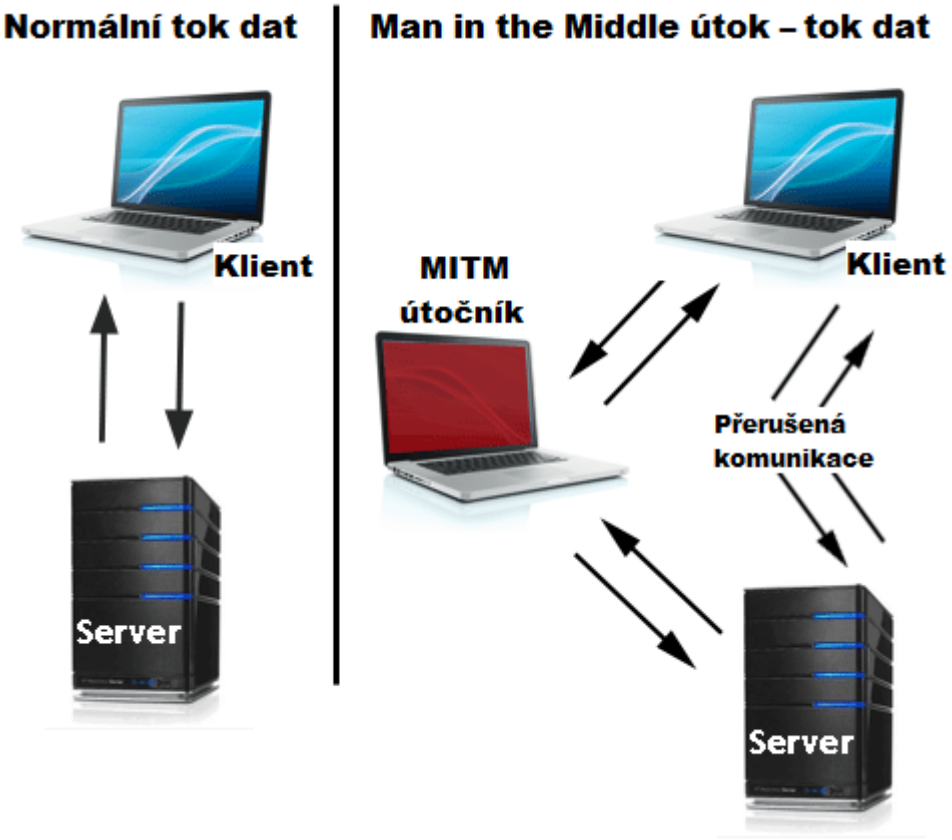
Při neopatrném zacházení s mobilním zařízením může nastat situace, kdy cizí člověk nahlédne přes rameno uživateli, přičemž uživatel samozřejmě o tomto neví. V lepším případě nepovolaná osoba zahlédne pouze část důležitých informací nebo útržky komunikace. V horším případě uživatel zadává přihlašovací údaje, které tak nedobrovolně poskytne útočníkovi. Další možností, jak zpřístupnit data neautorizované osobě je zapůjčení mobilního zařízení, např. někomu blízkému. Pro něj pak jsou citlivé informace prakticky na dosah ruky, pokud majitel mobilního zřízení v něm má uloženy přihlašovací údaje. Dopady neúmyslného zpřístupnění dat jsou podobné jako při krádeži nebo ztrátě, avšak pravděpodobnost zneužití dat a tedy celkové riziko jsou signifikantně menší.

Uživatelé si nejsou vždy vědomi veškerých funkcí mobilních zařízení a jejich aplikací. Často je požadováno, aby uživatel dal souhlas se shromažďováním osobních údajů před použitím dané funkce či aplikace, přesto při jejich použití zapomíná, že svůj souhlas poskytl a případně ani neví, pro jaká data byl souhlas poskytnut. Příkladem může být nahrávání souboru do vzdáleného uložiště. Součástí tohoto procesu je výběr souboru a výběrem souboru již uživatel dává souhlas, aby soubor mohl být nahrán, tedy mohlo s ním být manipulováno. Pokud takto nerozvážně uživatel zachází s firemními daty, tak se tato data mohou dostat do nesprávných rukou, nehledě na to, že z pohledu organizace se již jedná o nezabezpečená data (ENISA, 2010).

c) Hrozba používání nezabezpečených bezdrátových sítí

Mobilní technologie se vyznačují velmi vysokou konektivitou a lze je připojit k většině Wi-Fi sítí. Je nutné si však dát pozor na nezabezpečené bezdrátové sítě, ty totiž mohou být odposlouchávány a informace přenášené po této síti jsou mnohdy nešifrovaná a vystavena riziku. Na nezabezpečené síti je větší pravděpodobnost tzv. MITM (Man in the middle – člověk uprostřed) útoku. Princip spočívá v tom, že útočník odposlouchávající komunikaci přesměruje tok dat skrze sebe a tím se stane aktivním prostředníkem

v komunikaci. Tímto se mu naskýtá příležitost nejen odposlouchávat, ale obsah komunikace také měnit (NIST SP 800-124, 2013).



Obr. 2-3: Schéma MITM útoku a normální komunikace

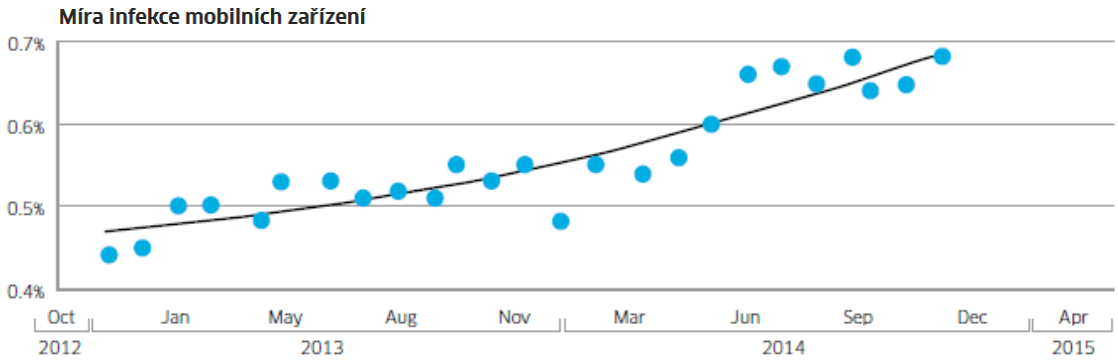
Zdroj: [http://www.veracode.com/security/man-middle-attack]

d) Hrozba napadení virem, spywarem nebo jiným škodlivým kódem

Stejně jako desktopové počítače nebo laptopy jsou mobilní zařízení náchylná k napadení virem, spywarem, trojským koněm nebo jiným typem škodlivého kódu či programu. Vzhledem k tomu, že v mobilních zařízeních se často nacházejí citlivá data nebo uložené přihlašovací údaje a existuje více možností jak zneužít zařízení oproti těm klasickým, stávají se mobilní zařízení pro útočníky více a více atraktivní, a proto hrozba napadení se stále zvyšuje.

To také potvrzuje studie společnosti Alcatel-Lucent (2015), která uvádí, že rychlost, s jakou jsou infikována mobilní zařízení, se stále zvětšuje. Nárůst infekcí v roce 2014 činil 25 % a v porovnání s rokem 2013, kdy byl „pouze“ 20% nárůst, lze předpokládat mírně zvyšující se trend i do budoucna (viz obr. 2-4). Koncem roku 2014 byla míra nakažení

malwarem 0,68 %, z tohoto čísla se odhaduje, že nakažených malwarem je přibližně 16 miliónů mobilních zařízení. Mezi 20 nejrozšířenějšími nákazami je 6 řadících se do kategorie spyware, což je software navržený tak, aby bez vědomí uživatele sbíral data ze zařízení. To také zahrnuje SMS zprávy, emailovou komunikaci, informace o kontaktech nebo údaje o prohlížených webových stránkách, tedy jak firemní, tak osobní data.



Obr. 2-4: Míra infekce mobilních zařízení od prosince 2012 do prosince 2014

Zdroj: ALCATEL-LUSCENT. *Motive Security Labs malware report – H2 2014* [online], https://resources.alcatel-lucent.com/asset/184652

Nejvíce ohrožena jsou ta mobilní zařízení, která běží pod operačním systémem Android, jelikož 99 % pozorovaných napadení se týká právě tohoto systému. Je to dáno tím, že Android je nejrozšířenějším mobilním operačním systémem. Zdrojem nákazy jsou nejčastěji aplikace stažené z různých zdrojů včetně oficiální distribuční sítě Google Play. Navíc oproti ostatním OS (nejen mobilním) je zranitelnější, tudíž snadnějším cílem, jelikož pomocí digitálních certifikátů aplikací je obtížné najít jejího vývojáře a také je poměrně snadné aplikaci určenou pro Android dekompilovat, vložit do ní vlastní zdrojový kód a zase digitálně podepsat (Alcatel-Luscent, 2015).

e) Hrozba zpracování nedůvěryhodného nebo nebezpečného obsahu

Mobilní zařízení se mohou setkat s různým obsahem prostřednictvím technologií, které pro jiná zařízení nejsou obvyklá. Praktickým příkladem jsou QR kódy (Quick response code – kód rychlé reakce), což jsou (ISO/IEC 18004:2015, 2015) kódy podobné těm čárovým, s tím rozdílem, že QR kód pracuje ve dvou rozměrech (využívá čtvercové matice, ve které jsou rozmístěny čtverce a podle jejich umístění se získává z kódu informace), nebo technologie NFC (ECMA-340, 2013), která umožňuje bezdrátovou komunikaci mezi dvěma aktivními (např. dvěma smartphony) nebo aktivním a pasivním (NFC zařízení bez napájení,

tzv. tag) přístrojem. V případě QR kódu jej stačí vyfotit pomocí fotoaparátu, kterým disponuje většina dnešních mobilních zařízení, a přístroj dekóduje informaci v něm obsaženou. Technologií NFC (Near field communication) pak disponuje menší množství přístrojů a informace se přenáší jejich dotekem nebo přiblížením na velmi krátkou vzdálenost.

Obě výše zmíněné technologie dokáží poskytnout různorodý obsah např. internetové odkazy, vizitky, nebo jiné textové informace. Problémem však je, že uživatel neví, jakou informaci se chystá načíst do zařízení, dokud není načtena a vyhodnocena. Odkazy mohou směřovat na stránky se škodlivým obsahem, zařízení se tak může stát terčem útoku a uživatel nemusí nic poznat. Tímto způsobem může útočník získat přístup k datům v zařízení nebo sledovat uživatelskou aktivitu (NIST SP 800-124, 2013).

f) Hrozba použití nedůvěryhodného zařízení

Na vysokých školách lze předpokládat tzv. BYOD (Bring your own device – dones si své zařízení) přístup, když se berou v úvahu mobilní zařízení, a z tohoto pohledu je nutné na každé zařízení pohlížet jako na nedůvěryhodné a nezabezpečené, když se připojuje do univerzitní počítačové sítě. Je třeba předpokládat, že zařízení může být napadeno škodlivým kódem. Mnohdy se uživatelé snaží prolomit výrobcem zabudovaná omezení operačního systému mobilního zařízení sami, v případě telefonů s OS Android se jedná o tzv. rootování, a u telefonů společnosti Apple, která ve svých zařízeních používá iOS se jedná o tzv. jailbreak. Tímto lze obejít nejen restrikce, ale také i různá bezpečnostní opatření zabudovaná v operačním systému a v konečném důsledku se zařízení stává zranitelnějším. V případě iOS to v minulosti, konkrétně do verze iOS 6, byla jediná možnost, jak instalovat do zařízení aplikace třetích stran (NIST SP 800-124, 2013).

Z výčtu hrozeb uvedených a popsaných výše je patrné, že mobilní zařízení představují pro organizaci nemalé bezpečnostní riziko, jehož zdrojem nemusí být jenom cizí člověk, útočník využívající zranitelnosti ze vzdáleného místa, ale také sám uživatel. Ve všech případech je nutno počítat s tím, že hodnota, důležitost a množství dat, kterých se hrozba týká, roste s postavením člověka v rámci organizace. V tomto kontextu je také důležité zmínit pojem „*konzumerizace*“. Ve své podstatě se jedná o zavádění technologií do korporátní sféry, které původně byly určeny pro spotřebitelský sektor. Základní myšlenkou konzumerizace je, že uživatelé mají přístup k širokému spektru technologií, zařízení a služeb mnohem vyspělejších, než ty, které jim mohou nabídnout IT oddělení samotných organizací. A v tom

tkví celý problém, jelikož lidem se osvědčilo používat tyto technologie pro osobní potřebu, zjistili, jaké možnosti se v tomto nacházejí a nevyhnutelně tedy chtějí tyto technologie používat i v zaměstnání. To z hlediska bezpečnosti znamená mnohem více typů zařízení, operačních systémů atd., a tím pádem více bezpečnostních rizik, které je třeba brát v úvahu (Madden, 2014).

Zde je velmi patrné, jak na sebe vzájemně působí integrita, dostupnost a důvěrnost informací, což jsou složky definice informační bezpečnosti (viz kapitola 1). Na jednu stranu uživatelé chtějí co nejvíce umožnit a zjednodušit přístup k informacím (přístup do firemních informačních systémů, podnikové elektronické poště, kalendáři a kontaktům apod.) a na stranu druhou IT specialisté se snaží data ochránit, mít kontrolu nad správou mobilních zařízení vstupujících do podnikové sítě nebo chránit firemní síť před nakaženým zařízením. V tomto ohledu výše zmíněná konzumerizovaná zařízení představují největší výzvu, jelikož nebyla primárně určena pro použití uvnitř organizace a sama o sobě nemají implementována potřebné bezpečnostní nástroje od výroby, přesto i na těchto zařízeních je nutné aplikovat bezpečnostní politiky organizace. Aby toho bylo možné dosáhnout, existuje několik možností, jak vynutit dodržování bezpečnostních politik, výše zmíněným hrozbám předcházet nebo zmírňovat jejich dopady a zároveň uživatelům umožnit využívat firemní prostředky v mobilních zařízeních (Sterk, 2014).

2.2.2 Enterprise Mobility Management (EMM)

Enterprise mobility management (Správa podnikové mobility) lze definovat jako přístup umožňující využívání mobilních zařízení zaměstnanci, který řeší otázky bezpečnosti, správy a řízení mobilních informačních technologií. Obecně se jedná o soubor lidí, procesů, politik, nástrojů a technologií, zabezpečujících práci s mobilními zařízeními uvnitř organizace (Madden, 2014).

EMM nástroje jako celek v sobě zahrnují kombinaci různých nástrojů, které mohou buď být součástí celku, nebo pracovat naprosto odděleně a nezávisle na sobě. Mezi základní složky EMM patří:

- MDM – Mobile Device Management (Správa mobilních zařízení),
- MAM – Mobile Application Management (Správa mobilních aplikací),

- MIM – Mobile Information Management

Mezi další nástroje, které EMM v sobě zahrnuje, je možné zařadit MEM – zkratka, která má více významů – Mobile Expense Management (Správa mobilních výdajů) a Mobile Email Management (Správa mobilní elektronické pošty), synchronizaci dokumentů a souborů ad. Z přístupů, které se v rámci EMM uplatňují, lze jmenovat již dříve zmíněný BYOD (viz kapitola 2.2.1, položka f)) a COPE (Corporate Owned, Personally Enabled – korporátně vlastněno, pro osobní potřebu povoleno), což je přístup, kdy zaměstnanec používá organizací vlastněné zařízení i pro své osobní potřeby, tedy přístup ve své podstatě opačný oproti BYOD (Sterk, 2014), (Madden, 2014).

Je vhodné zmínit se, že v minulosti bylo pro organizace zásadní spravovat pouze mobilní zařízení a jejich bezpečné připojení do počítačové sítě, což je úloha MDM nástrojů, avšak trend rostoucích nároků na správu mobilních aplikací, jejich bezpečné používání a mnoho dalších faktorů vedlo k tomu, že se více prosazují daleko komplexnější EMM řešení pokrývající širší okruh oblastí spojených s mobilní bezpečností.

2.2.3 Mobile Device Management (MDM)

Mobile device management je oblastí, která se zabývá nasazením, zabezpečením, monitorováním, začleněním a správou mobilních zařízení používaných v rámci organizace. MDM nástroje se starají zejména o prosazování bezpečnostních politik a nastavením mobilních zařízení. Důležité pro tyto nástroje je, že se nezaměřují pouze na úzký okruh výrobců zařízení a operačních systémů, ale orientují se na co možná největší množství zařízení. MDM je možné považovat za základní kámen EMM řešení (Sterk, 2014).

Aby bylo možné nasadit MDM řešení a pomocí něj pak bylo možné spravovat jednotlivá mobilní zařízení, je nutná přítomnost 3 základních komponent:

- je potřeba zařízení, které je možné spravovat,
- je potřeba protokolu umožňujícího vzdálenou správu (např. OMA Device Management protokol – OMA DM – což je otevřený standard implementovaný ve velkém množství mobilních zařízení a ve své podstatě je nezávislý na mobilní platformě),

- je potřeba serveru, na kterém budou nastavovány bezpečnostní politiky, a který tyto politiky bude v zařízeních řídit a prosazovat.

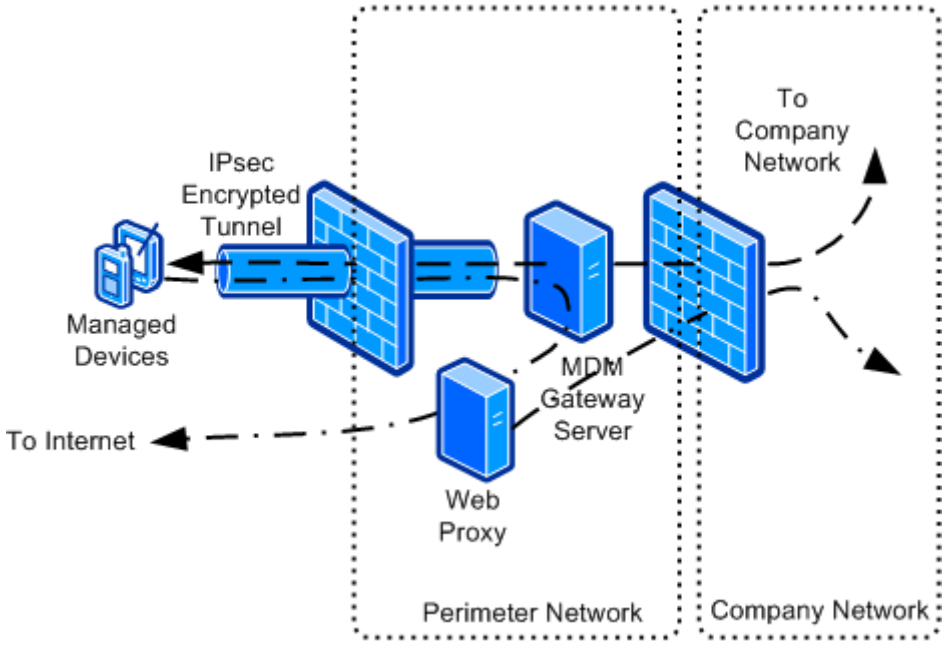
Z pohledu MDM je zařízení, které je možno spravovat, takové, u nějž lze měnit různá nastavení a funkce, vykonávat činnosti správy a dotazovat se na informace. Pro použití v organizaci to znamená, že u takového zařízení se dá nastavit např. bezdrátový a VPN přístup k síti, nakonfigurovat emailový klient, povolit šifrování či jiná nastavení bezpečnosti. Samozřejmě je možné krom počátečního nastavení přístroje vykonávat akce i přímo, jako jsou instalace a odstraňování aplikací, změna hesel nebo změny nastavení v případě úprav bezpečnostních politik. Velmi užitečná funkce, kterou MDM nástroje umožňují, je pak blokace přístroje, případně úplné vymazání dat z jeho interní, ale také externí, paměti. Dotazováním se na informace se zde rozumí to, že přímo v MDM systému lze zjistit velké množství informací o zařízení, tj. sériové číslo, IMEI, model, telefonní číslo, stav baterie nebo paměti, instalované aplikace, jeho umístění pokud to podporuje a mnoho dalších.

Nedílnou součástí provozu mobilního zařízení je jeho vzdálená správa, v mobilním světě tzv. OTA správa (Over-the-air, česky správa vzduchem nebo bezdrátová správa). Toto zaručuje, že není nutné zařízení přinášet zodpovědné osobě, ale veškeré úkony jsou prováděny centrálně. To velmi zvyšuje účinnost jednotlivých funkcí, které byly uvedeny v předchozím odstavci, a také zjednodušuje a zvyšuje účinnost samotné správy zařízení. Velmi dobrým příkladem použití vzdálené správy je, že pokud uživatel ztratí nebo je mu zcizen telefon, je možné se o jeho zablokování a vymazání postarat velmi rychle a zajistit tak, že firemní data se nedostanou do nepovolaných rukou (Madden, 2014).

Poslední důležitou komponentou je server, který se bude starat o bezpečnostní politiky. Samozřejmě je možné se o jednotlivá zařízení starat manuálně, avšak s jejich rostoucím počtem takový přístup ztrácí na efektivitě. Mobilní operační systémy již mají v sobě zabudovány běžné bezpečnostní opatření a politiky, ale MDM servery navíc umožňují nasadit vlastní specifická opatření a politiky, např. zákaz instalace určitých aplikací nebo instalace bezpečnostních certifikátů. Aby se zjednodušila správa veškerých zařízení, tak lze vytvářet a spravovat skupiny zařízení podle typu uživatelů. V tomto případě přijde vhod, že MDM servery mohou být začleněny přímo do IT infrastruktury a dokáží komunikovat a získávat informace z různých systémů v organizaci. Nutností je, aby server měl možnost

připojit se do sítě Internetu, bez tohoto by nebylo možné komunikovat vzdáleně s přístroji. Tím pádem musí být i server určitým způsobem zabezpečen, např. firewallem (Sterk, 2014).

Na Obr. 2-5 je příklad schématu jakým způsobem může fungovat MDM řešení, zejména z pohledu ze strany organizace. V tomto případě se jedná o System Center Mobile Device Manager společnosti Microsoft. Komunikace zde začíná tím, že mobilní zařízení vyšle požadavek na připojení do sítě pomocí VPN klienta. Brána po přijetí požadavku provede autorizaci a ověření zařízení a vytvoří se potřebné parametry pro VPN připojení. Poté mobilní zařízení odešle požadavek na přidělení nebo obnovení virtuální IP adresy a brána zkontroluje, zda se jde o jediné připojení tohoto zařízení, jelikož je povoleno maximálně jedno, a následně IP adresu přidělí. Poté již je zařízení připojeno do interní sítě a může využívat podnikových zdrojů (Microsoft Corp., 2009).



Obr. 2-5: Schéma MDM řešení společnosti Microsoft
Zdroj: (Microsoft Corp., 2009)

Z pohledu zařízení pak MDM řešení funguje tak, že na pozadí operačního systému běží aplikace, která se stará o vše potřebné, případně je nainstalován konfigurační profil, který provede nezbytná nastavení. Jak již bylo několikrát zmíněno, samotné mobilní operační systémy mají již zabudovány nějaké bezpečnostní opatření. Mezi takové patří i kontejnerizace aplikací, tj. že aplikace běží ve svém vyhrazeném prostoru, tzv. kontejneru, a mimo něj nemá přístup. Aby se vyřešila problematika BYOD přístupu, kdy uživatelé by byli velmi nespokojeni, kdyby jejich zařízení byla plně kontrolována organizací, tak byl podobný

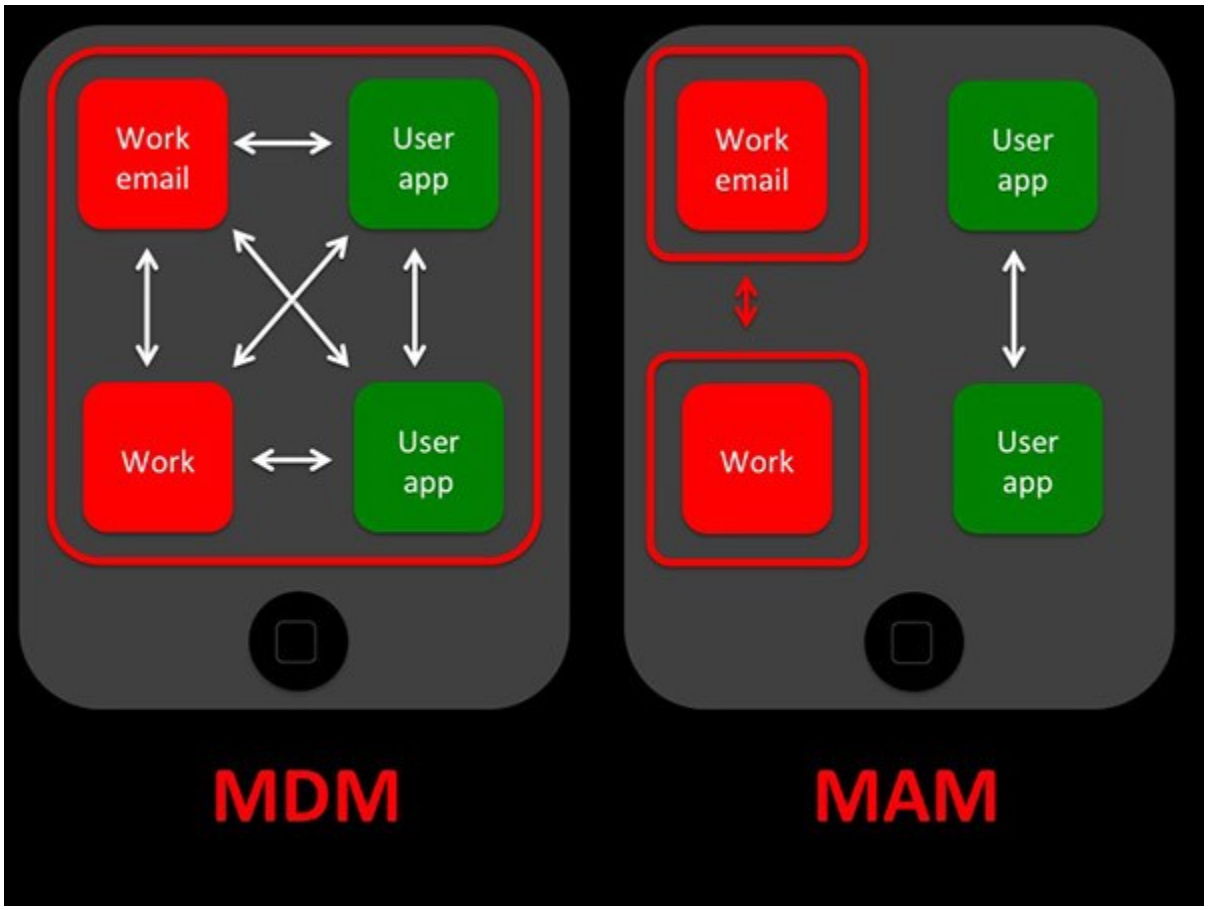
koncept zaveden i v rámci MDM. V zařízení, které není ve vlastnictví organizace, je tedy vytvořen kontejner, někdy také nazýván sandbox (pískoviště – prostor, ze kterého se písek nedostane ven, analogicky pak prostor, ze kterého se data nedostanou ven), pro firemní data, která jsou oddělena od osobních dat. To samé platí i pro aplikace a další prostředky. Tím se docílí toho, že zařízení není kontrolováno úplně celé a mimo kontejner nejsou aplikovány bezpečnostní politiky a opatření organizace. V takovém zařízení pak mohou být najednou vymazány veškerá data organizace, přičemž osobní prostor zůstane zachován. To je velmi výhodné v případě ukončení pracovního poměru.

V současném rychle se rozvíjejícím světě technologií je potřebné a žádoucí, aby MDM řešení a nástroje:

- byly kompatibilní s většinou běžně dostupných mobilních operačních systémů a aplikací,
- dokázaly pracovat přes různé poskytovatele služeb,
- mohly být nasazeny a spravovány vzdáleně a zacílené na určitá zařízení podle potřeby,
- dokázaly se rychle přizpůsobovat měnící a vyvíjející se nabídce operačních systémů a aplikací,
- mohly přidávat a odebírat v systému zařízení podle potřeby, čímž by se zajistil optimální výkon a bezpečnost sítě.

2.2.4 Mobile Application Management (MAM)

Mobile application management (správa mobilních aplikací) se zaměřuje výhradně na správu aplikací v zařízeních a jejich bezpečné dodávání, jedná se tedy o nižší stupeň kontroly nad zařízením oproti MDM, avšak vyšší stupeň kontroly aplikací. Správa aplikací je sice už funkce využívaná u MDM řešení, ale MAM zachází ještě podstatně dál. Rozdíl mezi MAM a MDM je možné pozorovat na obr. 2-6.



Obr. 2-6: Rozdíl v principu fungování MAM a MDM
Zdroj: [http://www.brianmadden.com/blogs/jackmadden/archive/2013/08/06/get-ready-for-ios7-by-learning-the-difference-between-3rd-party-and-platform-enabled-mam.aspx]

Způsob jakým jsou mobilním zařízením dodávány aplikace, je u všech mobilních platforem velmi podobný. Každá z platforem má svou vlastní distribuční síť aplikací, pro Android to je Google Play, pro iOS to je App Store, pro Windows Phone to je Windows Phone Store a v případě BlackBerry se jedná o BlackBerry World. V rámci jednotlivých distribučních sítí lze získat jak placené aplikace, tak aplikace zdarma a nejenže uživatel získává aplikace z jediného místa, ale i pro vývojáře aplikací je toto výhodné, jelikož nemusí využívat vlastních distribučních kanálů. S tím je však spojen jeden problém, i přestože jsou využívány bezpečnostní a kontrolní mechanismy, může se stát, že uživatel stáhne a nainstaluje potenciálně nebezpečnou aplikaci, a to je z pohledu organizace nežádoucí. MAM využívá takového principu doručování aplikací uživatelům prostřednictvím tzv. firemního obchodu s aplikacemi (Corporate Application Store). Zde je také využito principu kontejnerizace, ale na rozdíl od MDM je vytvořen aplikační kontejner, který striktně oddělí pracovní a soukromý prostor a tím zabezpečí chod aplikace před případným nebezpečným obsahem. Takto nejsou bezpečnostní opatření a politiky aplikovány na celé zařízení, ale pouze na samotné aplikace dodávané prostřednictvím firemního obchodu s aplikacemi. Zde je

důležité zmínit, že bezpečnostní politiky nelze vynutit u aplikací instalovaných z jiných než firemních zdrojů (Sterk, 2014).

Mobile application management není pouze o dodávání aplikací, na které se vztahují bezpečnostní opatření, ale jde v podstatě o kontrolu životního cyklu aplikací. MAM řešení mohou disponovat mnoha užitečnými vlastnostmi a mezi ně patří (Madden, 2014):

- dodávání aplikací prostřednictví firemního obchodu s aplikacemi,
- aktualizace aplikací,
- monitoring výkonu aplikací (a také hlášení o pádech a různých standardních i nestandardních událostech),
- sběr informací ohledně využívání jednotlivých aplikací
- správa uživatelských skupin, tj. komu budou instalovány jaké aplikace ad.

Nutno zmínit, že správa aplikací je také možná vzdáleně. Pravděpodobně je MAM model daleko vstřícnější k BYOD uživatelům, přece jen je pro uživatele mnohem přijatelnější fakt, že organizace nebude kontrolovat celé jejich zařízení, ale pouze některé aplikace.

2.2.5 Mobile Information Management (MIM)

Mobile information management (v doslovném překladu správa mobilních informací, ale v tomto případě se jedná spíš o data) se zaměřuje na aplikaci bezpečnostních politik na data, řízení přístupu k datům, jejich šifrování, zálohování a ochranu před ztrátou bez ohledu na to, jaká aplikace k nim přistupuje. Akronym MIM je poměrně zcestný, jelikož se jedná o správu dat nikoliv informací, avšak bylo by matoucí požívat zkratku MDM vícekrát, a tak bylo rozhodnuto, že bude lepší používat MIM. Občas je možné se také setkat s výrazem Mobile Content Management (MCM – správa mobilního obsahu). Ve své podstatě není MIM řešení nic jiného než firemní cloudové uložiště dat. Nutné tedy je, aby MIM bylo nasazeno spolu s MAM nebo MDM řešením, důvodem je zejména to, že MIM řeší pouze to, který uživatel bude přistupovat k datům, ale už ne to, které aplikace k datům mohou přistupovat (Madden, 2014).

2.2.6 Další EMM nástroje

Jak již bylo zmíněno, tak výše zmíněné technologie patří mezi základní pilíře EMM. Ale existuje více nástrojů a přístupů patřících do rodiny EMM, nýbrž se jedná o takové, které se zaměřují na specifičtější problematiky a neřeší firemní mobilitu komplexně. Na následujících řádcích budou některé z nich zmíněny a zběžně také popsány.

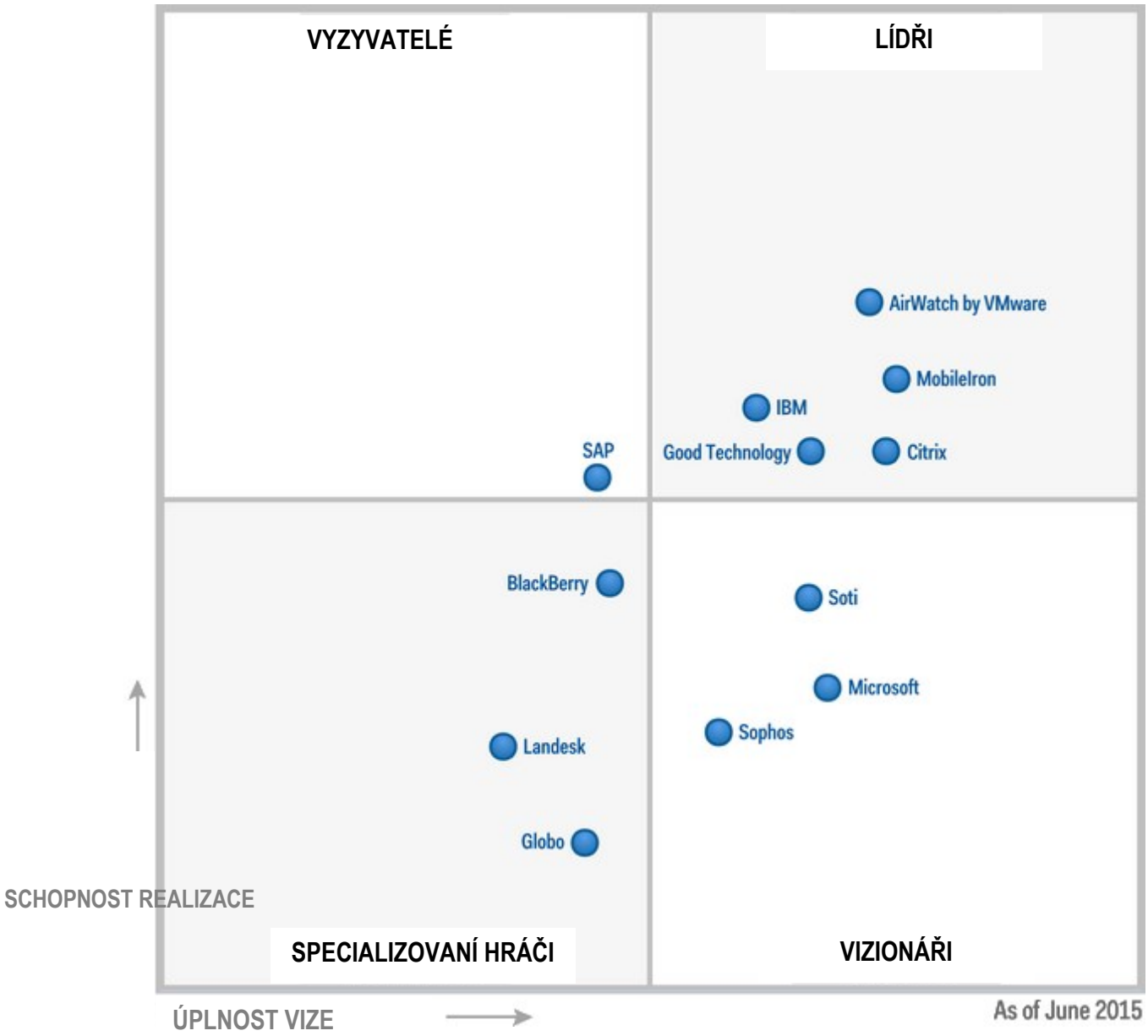
Mobile expense management (MEM, správa mobilních výdajů) jsou nástroje sloužící ke kontrole výdajů v souvislosti s používáním mobilních zařízení. Pomocí těchto nástrojů jsou zaměstnanci upozorňováni, pokud překročí určité limity a je i možné sledovat, kde by mohly být snižovány náklady. Tyto nástroje jsou využívány zejména u korporátně vlastněných zařízení, která mohou zaměstnanci používat i pro osobní účely.

Mobile email management (MEM, správa mobilní elektronické komunikace) se zaměřuje čistě na mobilní emailovou poštu a zejména na její zabezpečení. V rámci firemní emailové schránky se často nacházejí citlivé data a dokumenty, které je nutno chránit, používá se zejména šifrování.

Dalšími nástroji mohou být vlastní zabezpečení webových prohlížečů, a to zejména v případě, kdy organizace využívá webově orientované aplikace nebo samotná synchronizace dokumentů (Sterk, 2014).

2.2.7 Dodavatelé EMM řešení

Momentálně existuje již velké množství produktů, řešících problematiku firemní mobility. Aby se lépe orientovalo v nabídce všech řešení, vydává každoročně společnost Gartner studii, která hodnotí dodavatele či poskytovatele na základě toho, jak schopni jsou realizovat svou vizi ohledně řešení a podle vize samotné a následně je rozdělí do 4 skupin: vyzyvatelé, lídři, specializovaní hráči a vizionáři.



Obr. 2-7: Magický kvadrant pro EMM společnosti Gartner
Zdroj: (Gartner, Inc., 2015)

V roce 2015 proběhlo prozatím poslední zhodnocení všech dodavatelů. Dle studie existuje více než 100 prodejců EMM řešení, ale aby mohl být zařazen do magického kvadrantu, tak musí být splněno:

- prodejce musí mít příjmy za realizaci EMM řešení alespoň 12 milionů dolarů,
- prodejce musí mít alespoň 5 referencí od společností používajících jeho řešení,
- EMM řešení musí podporovat operační systémy iOS, Android a Windows Phone,

- v rámci řešení musí být přítomno MDM, MAM, které je schopno kontejnerizovat aplikace, a MCM.

Na Obr. 2-7 je několik společností, které byly zařazeny do magického kvadrantu. Všechny tyto společnosti v současné době patří mezi špičku v oblasti firemní mobility a dodávají sofistikované a účinné nástroje. Jednotlivá řešení tedy nabízejí funkce popsané v dřívějších kapitolách a odlišují se mezi sebou pouze v detailech, případně ve výkonnosti a spolehlivosti řešení. Mezi lídry v oboru byly zařazeny společnosti VMware s produktem AirWatch, IBM s produktem MaaS360, MobileIron se stejnojmenným produktem, Good Technology s produktem Good Dynamics Secure Mobility Platform a Citrix s produktem XenMobile (Gartner, Inc., 2015).

2.2.8 Možnosti nasazení EMM a faktory, které je třeba zohlednit

Každá organizace používá mobilní zařízení různým způsobem, a tedy není vždy výhodné a ani nutné nasadit veškeré možnosti, které EMM nabízí. Je třeba zohlednit několik faktorů, které hrají důležitou roli při výběru správného řešení, mezi ně patří:

- Email – pravděpodobně bude využíván všemi společnostmi, ale otázkou je, jakým způsobem bude provozován. Je třeba se zaměřit na to, zda bude použit vestavěný emailový klient nebo klient vytvořený EMM dodavatelem, anebo zda bude použito šifrování příloh.

- Bude třeba spravovat přímo zařízení, anebo stačí spravovat firemní aplikace? Podle toho se určí, zda využívat MDM nebo MAM.

- Budou moci uživatelé používat svá vlastní zařízení (BYOD), anebo budou v rámci organizace pouze firemní zařízení (COPE)?

- Osobní aplikace – budou moci uživatelé instalovat a používat veškeré aplikace volně nebo pouze povolené předem povolené a v tomto případě, jakým způsobem budou schvalovány?

- Firemní aplikace – bude nutné používat vlastní firemní aplikace?

- Prostředí firemních aplikací – budou moci aplikace mezi sebou určitým způsobem komunikovat (kopírování textu apod.)? Bude možné používat jednotného přihlášení, a tedy při použití jedné aplikace již nebude nutné se přihlašovat do jiných?

Podle toho jaké budou odpovědi u výše položených otázek, je možné aplikovat EMM řešení mnoha různými způsoby, s různým stupněm zabezpečení apod. Je jisté, že ať už bude využito jakékoliv možnosti, tak každá z nich má své výhody a nevýhody, nehledě na to, že čím komplexnější a sofistikovanější řešení bude, tím více se promítne do nákladů (a to jak za vybudování řešení, tak i za jeho provoz). Mezi základní scénáře je možné zařadit (Madden, 2014):

- Použití MDM s množstvím omezujících bezpečnostních opatření – takové řešení je výhodné při použití zařízení vlastněných organizací, případně když se o jedno zařízení dělí více uživatelů. V zařízení většinou není povoleno instalovat vlastní aplikace ani používat jakýkoliv soukromý obsah.

- MDM s malým množstvím mírných bezpečnostních opatření – tento přístup je podobný předchozímu s tím rozdílem, že uživatel není vázán tolika pravidly. Na druhou stranu je takové řešení méně bezpečné (zejména nezabezpečené osobní aplikace mohou zapříčinit únik citlivých dat) kvůli nižšímu stupni kontroly nad zařízením. Zde se může jednat jak o BYOD, tak i COPE zařízení.

- MDM a MAM s využitím nativního emailového klienta – zde už se jedná o poměrně komplexní řešení zajišťující poměrně dobrou bezpečnost. Nevýhodou je pouze to, že emailové přílohy nejsou šifrovány a jsou tedy vystavovány riziku.

- MDM a MAM s využitím emailového klienta třetí strany – v podstatě se jedná o stejné řešení, ale emailový klient je ve většině případů zabezpečen a přílohy jsou chráněny. Na druhou stranu lidé jsou často zvyklí používat nativního klienta a nový nástroj jim nemusí vyhovovat.

- MDM a MAM s využitím šifrování emailových příloh – toto je kombinace, která v sobě spojuje výhody obou předchozích scénářů. Lidé používají to, na

co jsou zvyklí a zároveň přílohy jsou chráněny. Nevýhodou je, že firemní aplikace musí být psány tak, aby mohly pracovat se šifrovanými přílohami. Navíc texty emailové komunikace, kalendář, kontakty ad. jsou vystaveny osobním aplikacím.

- Samotné MAM – tento scénář bude použit zejména při využívání BYOD přístupu. Bohužel organizace nebude mít žádnou kontrolu nad zařízením, bude možné pouze kontrolovat firemní aplikace a jejich data.

2.2.9 Shrnutí

Správa podnikové mobility nabízí širokou paletu nástrojů pro řízení bezpečnosti mobilních zařízení uvnitř organizace a na trhu je dostupné velké množství řešení, která se o toto postarají. Také jak bylo zmíněno, je možné k podnikové mobilitě přistupovat mnoha způsoby, které mají různé výhody a nevýhody a také se odlišně projeví v nákladech. Správné EMM řešení ve výsledku snižuje riziko většiny hrozeb uvedených v kapitole 2.2.1. Riziko hrozby ztráty zařízení je řešena pomocí vzdáleného vymazání zařízení, při používání nezabezpečených bezdrátových sítí je využíváno šifrování dat na zařízení, před škodlivým obsahem a jeho zpracováním chrání firemní síť serverový firewall, antivir apod. a hrozba používání nedůvěryhodného zařízení již v podstatě nehrozí, jelikož zařízení jsou zavedena v systému. Bohužel hrozbu neúmyslného zpřístupnění citlivých dat nelze úplně vyřešit softwarovými a hardwarovými nástroji, ale riziko s ní spojené lze výrazně snížit např. vhodným školením.

Když jsou brány v potaz univerzity a vysoké školy, je nutné přihlédnout k tomu, že studentů je několikanásobně více než zaměstnanců, a proto je třeba počítat s velkým množstvím BYOD zařízení. Problematiku mobility na vysokých školách je tedy možné řešit hned několika způsoby a za přijatelné lze považovat kombinaci MDM, které nebude striktní a bude využívat principu kontejnerizace, a MAM, které studentů i zaměstnancům umožní používat potřebné aplikace. Z dostupných zdrojů lze zjistit, že univerzity České republice prozatím žádné EMM řešení nevyužívají, ale většinou umožňují mobilním zařízením připojit se do své vnitřní sítě pomocí VPN klienta. Na druhou stranu množství zahraničních univerzit již začalo řešit problematiku mobilních zařízení, např. Stanfordova univerzita zavedla MDM řešení schopné pracovat s operačními systémy iOS a Android, nebo Forhamská soukromá

univerzita, která MDM řešení aplikuje na zařízení ve svém vlastnictví, a která jsou poskytnuta zaměstnancům pro osobní i pracovní účely.

3 ANALÝZA SOUČASNÉHO STAVU INFORMAČNÍ BEZPEČNOSTI NA VŠ

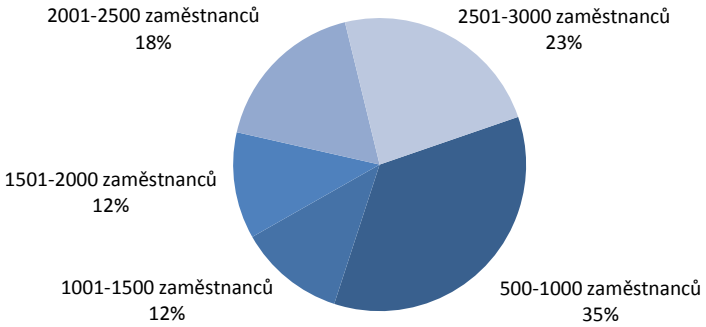
Analýza současného stavu informační bezpečnosti byla provedena na základě dotazníkového šetření, které proběhlo v prvním čtvrtletí roku 2015. Průzkumu se zúčastnilo celkem 18 veřejných vysokých škol a univerzit z České republiky, přičemž data byla anonymizována. Jednotlivé otázky dotazníkového šetření lze rozdělit do tří kategorií, otázky zaměřené na samotné respondenty a vysoké školy, otázky zaměřené na organizační bezpečnost a otázky zaměřené na síťovou bezpečnost. Vzhledem k povaze otázek nebyly některé otázky jednotlivými respondenty zodpovězeny a při vyhodnocování otázky pak nebyli tito respondenti započítáni.

3.1 Struktura respondentů

Začátek dotazníkového šetření byl věnován otázkám ohledně počtu studentů velikosti a typu vysokých škol a univerzit, které se průzkumu zúčastnily a také respondentům, kteří na tyto otázky odpovídali.

Otázka č. 1: Kolik zaměstnanců má Vaše vysoká škola/univerzita?

V průzkumu jsou nejvíce zastoupeny (35 %) vysoké školy zaměstnávající ne více než 1000 lidí. Druhou nejpočetnější kategorií jsou vysoké školy s 2501–3000 zaměstnanci. Dohromady tyto dvě kategorie představují více než polovinu (55 %) respondentů.

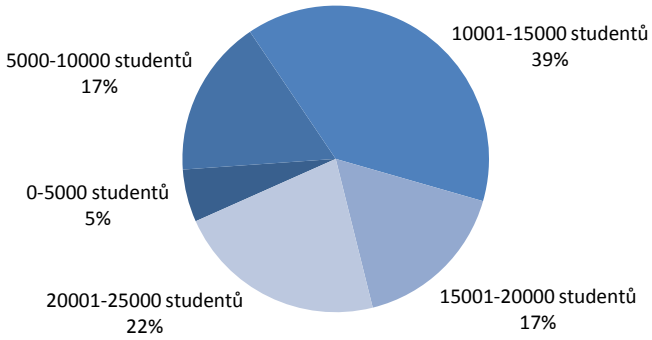


Graf 3-1: Kolik zaměstnanců má Vaše vysoká škola/univerzita?

Zdroj: vlastní zpracování

Otázka č. 2: Kolik studentů všech typů studia na Vaší vysoké škole/univerzitě studuje?

Největší podíl vysokých škol uvádí, že v rámci jejich studijních programů studuje od 10 do 15 tisíc studentů. Celkově v průzkumu převládají univerzity, na kterých studuje více než 10 001 studentů.

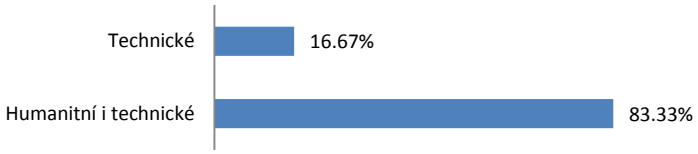


Graf 3-2: Kolik studentů všech typů studia na Vaší vysoké škole/univerzitě studuje?

Zdroj: vlastní zpracování

Otázka č. 3: Jaké obory studia nabízíte na Vaší vysoké škole/univerzitě?

V průzkumu převládají univerzity, které nabízejí jak technické, tak humanitní obory. V průzkumu vůbec nefigurují instituce poskytující pouze humanitní obory. Všechny dotazované instituce tedy nabízejí technické obory.

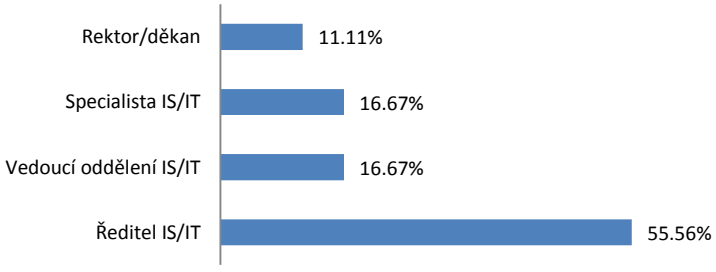


Graf 3-3: Jaké obory studia nabízíte na Vaší vysoké škole/univerzitě?

Zdroj: vlastní zpracování

Otázka č. 4: Jaká je Vaše pozice v rámci vysoké školy/univerzity?

Za více než polovinu vysokých škol účastnících se průzkumu odpovídali IT ředitelé. V drtivé většině pak odpovídali lidé, kteří jsou přímo napojeni na fungování IS/ICT.



Graf 3-4: Jaká je Vaše pozice v rámci vysoké školy/univerzity?

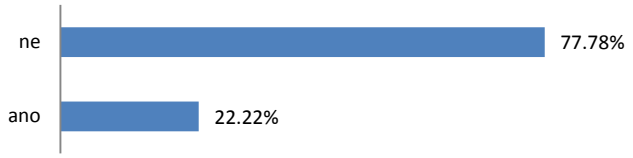
Zdroj: vlastní zpracování

3.2 Otázky organizační bezpečnosti

Informační bezpečnost není pouze o zabezpečení IS/ICT pomocí technických (hardwarových a softwarových) nástrojů. Z hlediska řízení bezpečnosti je také důležitá organizační neboli administrativní bezpečnost, která má na starost ustanovení povinností, kompetencí osob v organizace a jejich odpovědnost.

Otázka č. 5: Věnuje se některý pracovník Vaší organizace informační bezpečnosti jako hlavní pracovní náplni?

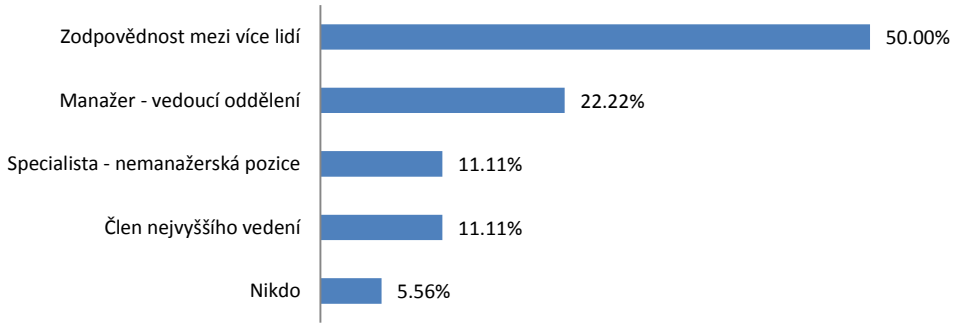
Většina respondentů (téměř 78 %) uvedla, že nemají vyhrazeného pracovníka zaměřeného primárně na informační bezpečnost.



Graf 3-5: Věnuje se některý pracovník Vaší organizace informační bezpečnosti jako hlavní pracovní náplni?
Zdroj: vlastní zpracování

Otázka č. 6: Kdo je na Vaší vysoké škole/univerzitě zodpovědný za řešení informační bezpečnosti?

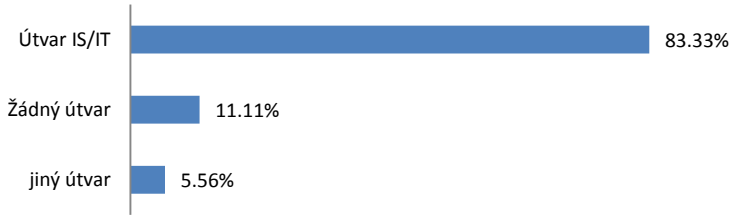
Zodpovědnost za informační bezpečnost je v polovině případů rozdělena mezi více lidí, což by mohlo naznačovat, že na různé oblasti bezpečnosti jsou dosazování různě zaměření specialisté z oblasti bezpečnosti. V necelé polovině případů pak za bezpečnost zodpovídá jeden pracovník, přičemž se nemusí jednat o odborníka z IT.



Graf 3-6: Kdo je na Vaší vysoké škole/univerzitě zodpovědný za řešení informační bezpečnosti?
Zdroj: vlastní zpracování

Otázka č. 7: Který útvar je zodpovědný za informační bezpečnost na Vaší vysoké škole/univerzitě?

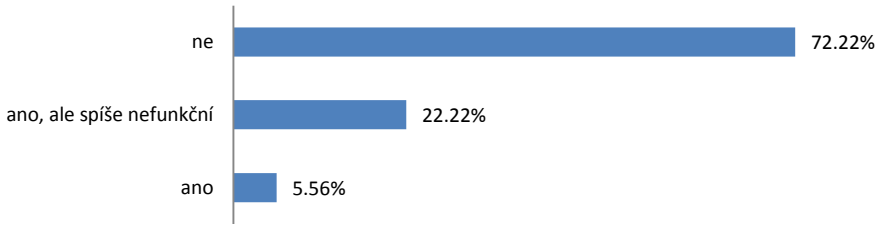
V naprosté většině případů se o informační bezpečnost stará útvar IS/IT, což je pochopitelné. Na jednu stranu je výhodou, že se o bezpečnost starají lidé, kteří ji dokáží zajistit zejména z technického hlediska, což by ve výsledku mohlo znamenat přílišnou restriktivní bezpečnostní politiku.



Graf 3-7: Který útvar je zodpovědný za informační bezpečnost na Vaší vysoké škole/univerzitě?
Zdroj: vlastní zpracování

Otázka č. 8: Existuje na Vaší vysoké škole/univerzitě funkční program zvyšování povědomí zaměstnanců v oblasti informační bezpečnosti (nikoliv BOZP)?

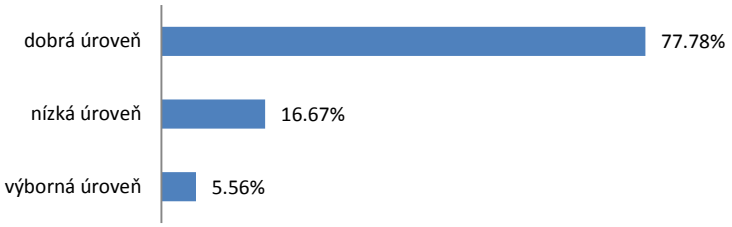
Na téměř třech čtvrtinách škol neexistuje žádný program, který by školil zaměstnance v oblasti informační bezpečnosti, a to i přesto, že chyby uživatelů bývají velice častou příčinou incidentů.



Graf 3-8: Existuje na Vaší vysoké škole/univerzitě funkční program zvyšování povědomí zaměstnanců v oblasti informační bezpečnosti (nikoliv BOZP)?
Zdroj: vlastní zpracování

Otázka č. 9: Jak hodnotíte vlastní úroveň řešení bezpečnosti?

Samotné instituce většinou hodnotí svou vlastní úroveň zabezpečení jako dobrou. Zde je však nutno brát v úvahu, že odpovědi jsou velice subjektivního rázu a předem nelze tvrdit, že úroveň zabezpečení je opravdu dobrá.

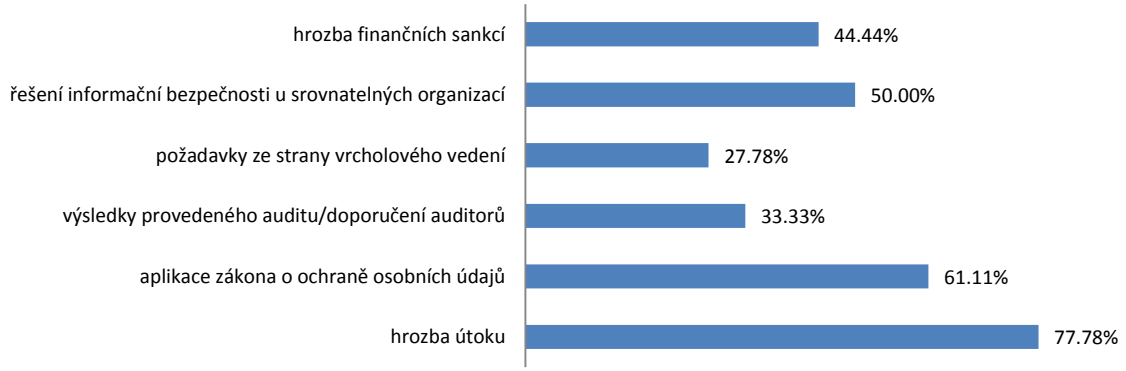


Graf 3-9: Jak hodnotíte vlastní úroveň řešení bezpečnosti?

Zdroj: vlastní zpracování

Otázka č. 10: Faktory, které mají největší vliv na prosazování informační bezpečnosti na vysokých školách.

Motivace, proč prosazovat informační bezpečnost je bezesporu důležitým aspektem, jelikož pak lze předpokládat, že bezpečnosti bude věnována dostatečná pozornost. Z výsledků je patrné, že nejvýznamnějším faktorem je hrozba útoku následovaný aplikací zákona o ochraně osobních údajů. Oba tyto faktory mají vliv u více než poloviny vysokých škol. V podstatě se nejedná o nijak překvapivé zjištění, jelikož hrozba útoku je velmi nebezpečným jevem a v nedávné minulosti bylo zaznamenáno nemalé množství hackerských útoků, a to i na organizace, u kterých lze předpokládat velmi dobré zabezpečení jednotlivých systémů. Z pohledu univerzit pak podle zákona o ochraně osobních údajů lze ukládat nemalé finanční sankce (přičemž hrozba finančních sankcí, jako samostatný faktor je až na 4. Pozici).

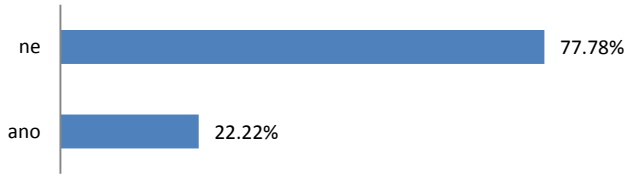


Graf 3-10: Faktory, které mají největší vliv na prosazování informační bezpečnosti na vysokých školách

Zdroj: vlastní zpracování

Otázka č. 11: Má Vaše vysoká škola/univerzita ve formě dokumentu formálně definovanou a nejvyšším vedením přijatou bezpečnostní politiku?

Definovanou bezpečnostní politiku má přibližně pouze necelá čtvrtina respondentů, což lze považovat za velmi malé číslo.

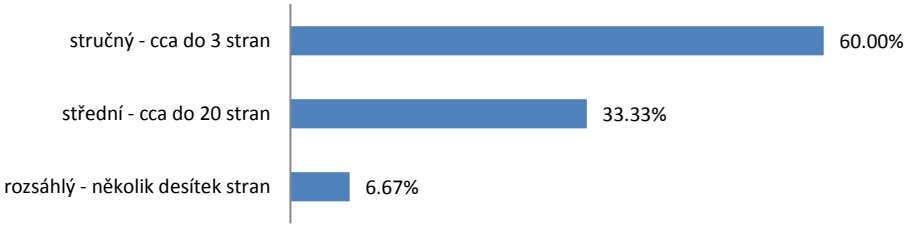


Graf 3-11: Má Vaše vysoká škola/univerzita ve formě dokumentu formálně definovanou a nejvyšším vedením přijatou bezpečnostní politiku?

Zdroj: vlastní zpracování

Otázka č. 12: Jaký je rozsah dokumentu bezpečnostní politiky?

I přestože téměř na pětině univerzit není schválená bezpečnostní politika, tak v drtivé většině případů je používán alespoň nějaký dokument definující bezpečnostní politiku, ačkoliv nebyl oficiálně schválen. V 60 % se pak jedná o poměrně stručný dokument s délkou do 3 stran.



Graf 3-12: Jaký je rozsah dokumentu bezpečnostní politiky?

Zdroj: vlastní zpracování

Otázka č. 13: Jak často dochází k aktualizaci dokumentu bezpečnostní politiky?

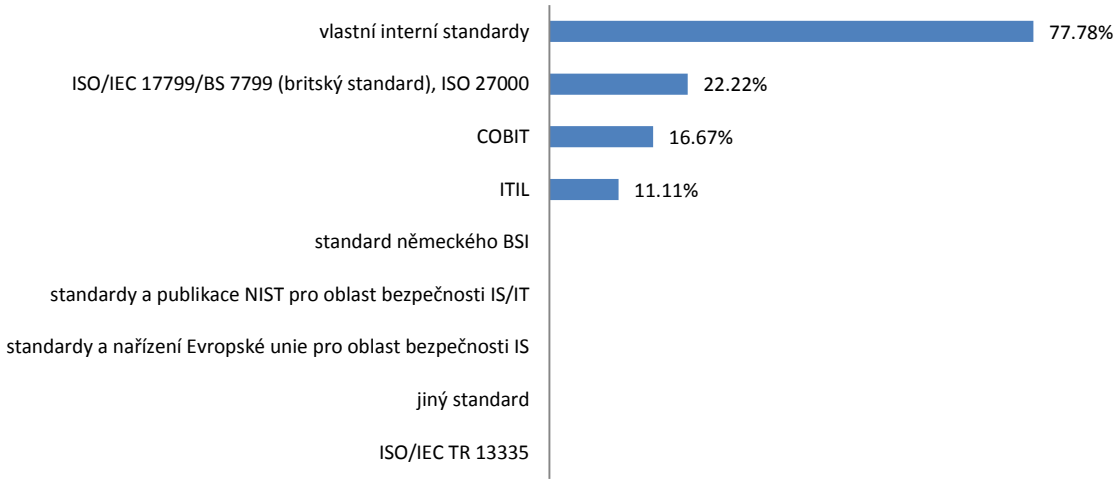
Ve většině případů probíhá aktualizace dokumentu bezpečnostní politiky nepravidelně, pouze podle potřeby. Pravidelná aktualizace tohoto dokumentu v přiměřeném intervalu, je však velice důležitá. Důvodem je poměrně rapidní vývoj informačních a komunikačních technologií, čímž se mění kybernetické prostředí a zvětšuje portfolio hrozeb. Aktualizací dokumentu bezpečnostní politiky se pak docílí toho, že i ve stále se vyvíjejícím prostředí bude možno adekvátně reagovat na nové hrozby. Znepokojující je, že ve 40 % případů tento dokument není vůbec aktualizován měnícím se potřebám informační bezpečnosti.

Graf 3-13: Jak často dochází k aktualizaci dokumentu bezpečnostní politiky?

Zdroj: vlastní zpracování

Otázka č. 14: Jaké mezinárodní standardy v oblasti informační bezpečnosti a/nebo IT governance jsou v rámci Vaší vysoké školy/univerzity využívány při řešení informační bezpečnosti?

Většina respondentů využívá při řešení informační bezpečnosti vlastní interní standardy a směrnice. Zajímavé je, že množství respondentů, u kterých existuje bezpečnostní politika na univerzitě, je stejné jako množství respondentů, kteří uvádějí využití standardu ISO 27000 (ISO/IEC 17799/BS 7799), jehož je bezpečnostní politika součástí, avšak ne vždy se jedná o ty stejné univerzity.

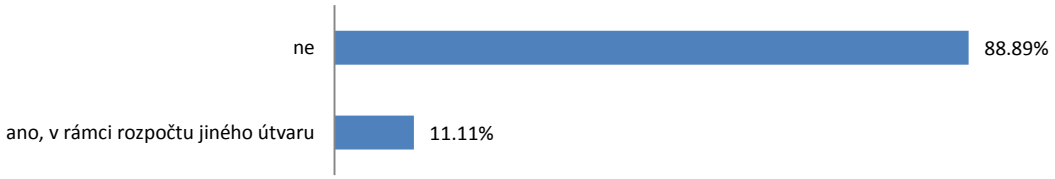


Graf 3-14: Jaké mezinárodní standardy v oblasti informační bezpečnosti a/nebo IT governance jsou v rámci Vaší vysoké školy/univerzity využívány při řešení informační bezpečnosti?

Zdroj: vlastní zpracování

Otázka č. 15: Má Vaše vysoká škola/univerzita vyčleněný samostatný rozpočet pro financování informační bezpečnosti?

Finanční prostředky jsou nezbytným zdrojem pro zajištění informační bezpečnosti, avšak pouze 11% respondentů uvedlo, že jejich univerzita má vyhrazeny finance výhradně pro tuto oblast.



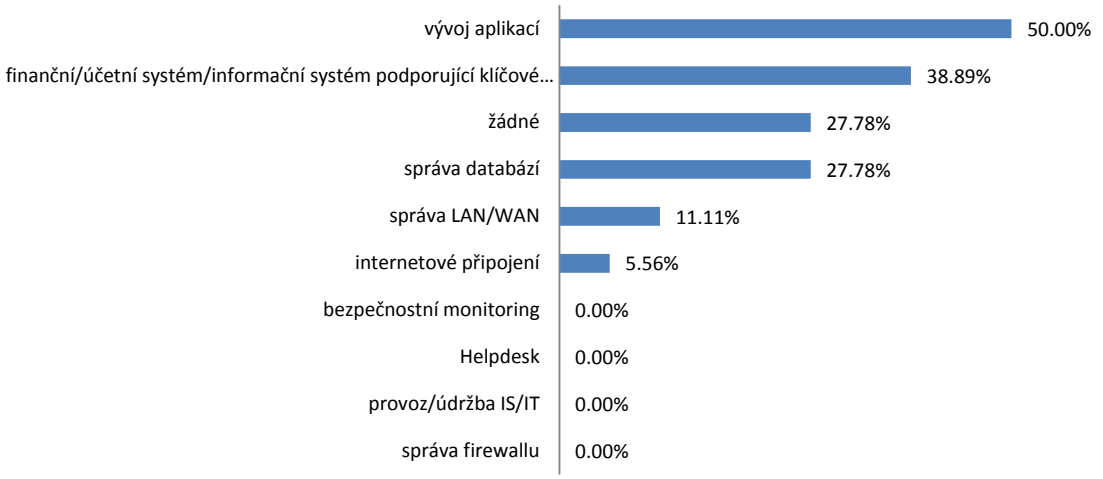
Graf 3-15: Má Vaše vysoká škola/univerzita vyčleněný samostatný rozpočet pro financování informační bezpečnosti?
Zdroj: vlastní zpracování

3.3 Otázky síťové bezpečnosti

Poslední část dotazníku byla zaměřena na otázky síťové bezpečnosti, tedy jakými technickými prostředky je zajištěna.

Otázka č. 16: Jaké části IS/IT outsourcujete (alespoň částečně) na Vaší vysoké škole/univerzitě?

Nejčastěji v současném univerzitním prostředí je outsourcován vývoj aplikací. Druhou skupinou, u které se využívá služeb externích dodavatelů, jsou různé informační systémy, jejichž podíl je přibližně stejný jako v minulém průzkumu. Avšak oproti roku 2012 se množství oblastí přesunulo pod správu samotných univerzit a celkový poměr externě zajištěných služeb se podstatně snížil. Navíc některé části IS/IT (bezp. monitoring, helpdesk, provoz a údržba IS/IT a správa firewallu) jsou spravovány pouze samotnými univerzitami. V roce 2012 se o celou infrastrukturu IS/IT starala pouze desetina univerzit, v současnosti už to je více než čtvrtina.

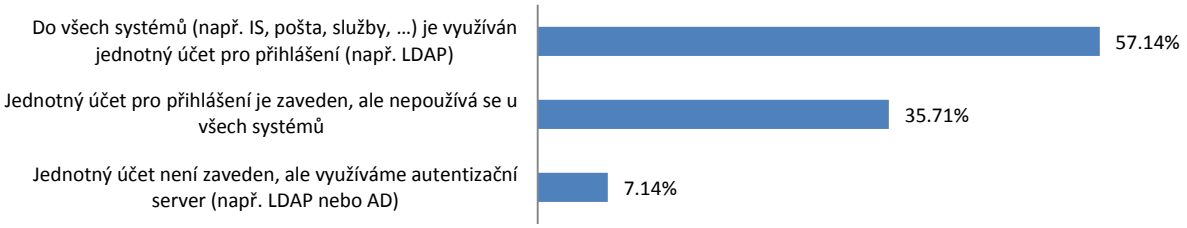


Graf 3-16: Jaké části IS/IT outsourcujete (alespoň částečně) na Vaší vysoké škole/univerzitě?

Zdroj: vlastní zpracování

Otázka č. 17: Jaký využíváte systém řízení uživatelských účtů?

Mnohdy je na univerzitách využíváno více informačních systémů, ke kterým přistupují jak studenti, tak zaměstnanci. Jednotné přihlašování (SSO – Single sign-on) je nejen přínosné pro uživatele, jelikož si nemusí pamatovat přihlašovací údaje pro každý systém zvlášť, ale také i z hlediska bezpečnosti. Podstatou SSO je, že přihlašovací údaje jsou uloženy na jednom místě centrálně a samotné systémy a služby k nim nemají přímý přístup, což výrazně napomáhá bezpečnosti. Navíc tím, že uživatel nemusí heslo psát vícekrát, se bezpečnost také zvyšuje. V tomto ohledu lze konstatovat, že zabezpečení je mezi univerzitami velice dobré, jelikož v omezeném rozsahu jednotné účty využívá více než 90 % vysokých škol a ve více než polovině je jednotný účet zaveden do všech systémů.



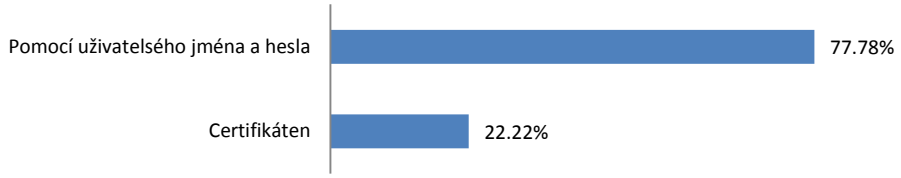
Graf 3-17: Jaký využíváte systém řízení uživatelských účtů?

Zdroj: vlastní zpracování

Otázka č. 18: Jakým způsobem jsou uživatelé při přístupu přes VPN ověřování?

Většina vysokých škol (nelze konstatovat, že všechny, jelikož ve 3 případech nebyla odpověď zjištěna) umožňuje připojení do vnitřní sítě z veřejné (nedůvěryhodné) počítačové sítě (např. internet) pomocí VPN. VPN mezi dvěma koncovými body veřejné sítě vytváří připojení simulující privátní síť, kdy přenášená data jsou šifrována, a toto připojení lze považovat za důvěryhodné a bezpečné. Zabezpečení tohoto připojení je na většině vysokých

škol zajištěno pomocí přihlašovacích údajů, což je jen o něco slabší zabezpečení než v případě použití certifikátů.

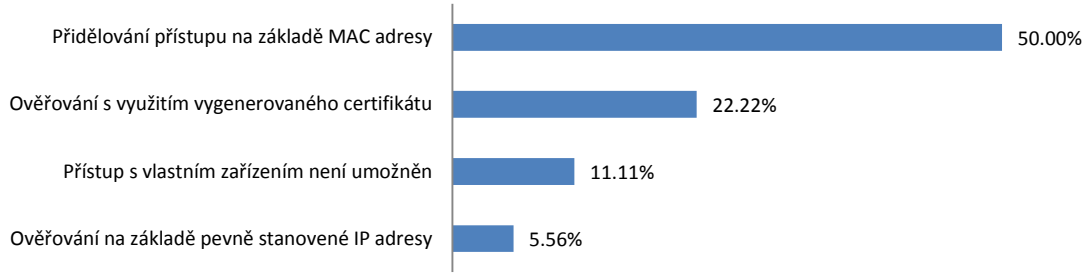


Graf 3-18: Jakým způsobem jsou uživatelé při přístupu přes VPN ověřování?

Zdroj: vlastní zpracování

Otázka č. 19: Způsoby přidělování oprávnění pro přístup k lokální síti s vlastním zařízením (připojení zařízení pomocí kabelu)?

Přístup do počítačové sítě s využitím UTP kabelu, je na většině vysokých škol umožněn, s tím, že nejčastěji se pro poskytnutí přístupu využívá kontroly MAC adresy síťové karty, což je jednoznačný identifikátor. Avšak toto zabezpečení lze obejít, jelikož existuje možnost změny MAC adresy softwarovým způsobem, tzv. MAC spoofing (podvržení MAC adresy). V tomto případě však útočník musí nějakým způsobem získat MAC adresu, která je zavedena v systému, nahodilé zjištění takové adresy prakticky není možné vzhledem k délce MAC adresy – 48 bitů (2^{48} možných kombinací).

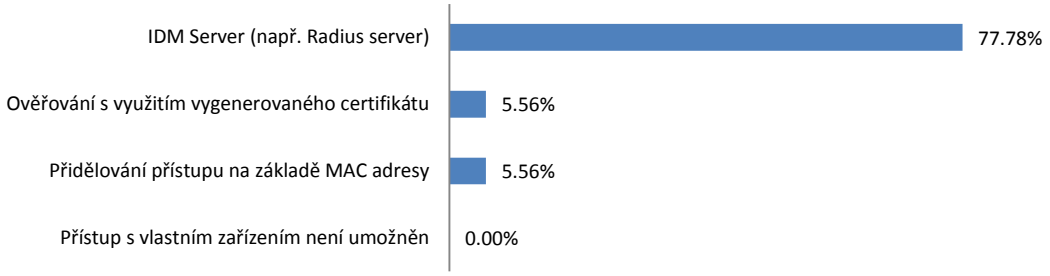


Graf 3-19: Způsoby přidělování oprávnění pro přístup k lokální síti s vlastním zařízením (připojení zařízení pomocí kabelu)?

Zdroj: vlastní zpracování

Otázka č. 20: Jakými způsoby probíhá přidělování oprávnění pro přístup k Wi-Fi síti s vlastním zařízením?

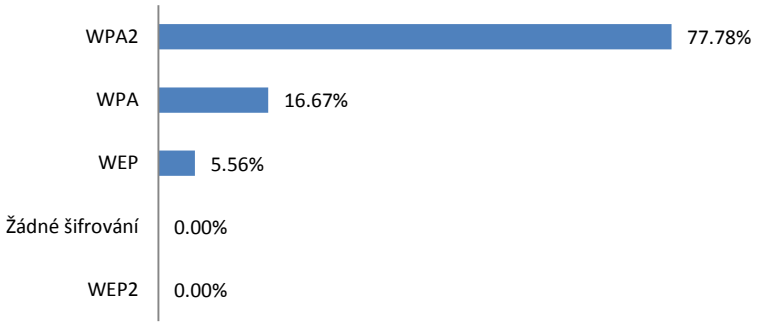
V rámci vysokých škol je vždy možné využít připojení k Wi-Fi síti. Pro přidělování oprávnění k těmto sítím využívá většina vysokých škol Identity management Server.



Graf 3-20: Jakými způsoby probíhá přidělování oprávnění pro přístup k Wi-Fi síti s vlastním zařízením?
Zdroj: vlastní zpracování

Otázka č. 21: Jaký typ šifrování komunikace využíváte ve Wi-Fi síti?

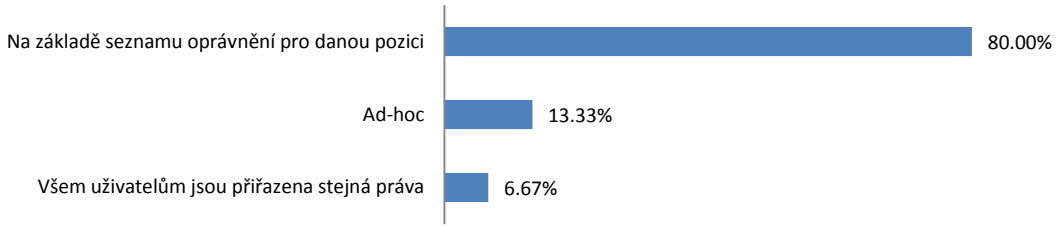
Komunikace v rámci bezdrátových sítí na vysokých školách je vždy šifrována. Na většině univerzit je používáno WPA2, případně WPA, zabezpečení, které je v současnosti více než dostačující. Stále je však možné setkat se s WEP zabezpečením, které je dosti nevyhovující, jelikož jeho šifrování bylo prolomeno v roce 2001.



Graf 3-21: Jaký typ šifrování komunikace využíváte ve Wi-Fi síti?
Zdroj: vlastní zpracování

Otázka č. 22: Přidělování práv k uživatelským účtům

Databáze a informační systémy univerzit obsahují data, která mají různou úroveň důvěrnosti. V tomto případě je žádoucí, aby přístup k takovým datům byl nějakým způsobem řízen a jednotlivým uživatelům či uživatelským skupinám byl přidělován přístup a práva pouze k datům, která jsou nutná pro výkon jejich pracovních činností.

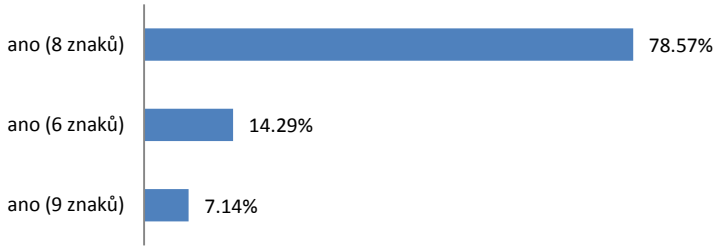


Graf 3-22: Přidělování práv k uživatelským účtům

Zdroj: vlastní zpracování

Otázka č. 23: Je stanovena minimální délka hesla pro přístup k uživatelskému účtu?

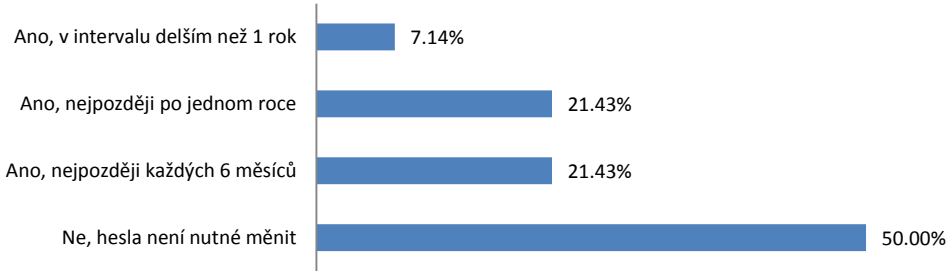
Délka hesla je jedním z faktorů, pomocí kterého se určuje síla hesla. Platí, že čím delší heslo je, tím je silnější a pro útočníky hůře zjistitelnější. Názor na doporučenou délku se často liší, vždy záleží na systému a např. zda jsou v hesle povoleny velká a malá písmena nebo číslice a speciální znaky. Takovou optimální hodnotou je délka kolem 8 znaků. Z průzkumu vyplývá, že na většině vysokých škol je systémem vyžadováno heslo právě o minimální délce 8 znaků.



Graf 3-23: Je stanovena minimální délka hesla pro přístup k uživatelskému účtu?
Zdroj: vlastní zpracování

Otázka č. 24: Mají uživatelé povinnost v pravidelných intervalech měnit svá hesla?

Pravidelně aktualizované heslo patří k zásadám, které zvyšují informační bezpečnost. Čím častěji se heslo mění, tím více se snižuje riziko jeho zneužití. V různých časových intervalech je po uživatelích vyžadována změna hesla na polovině vysokých škol.

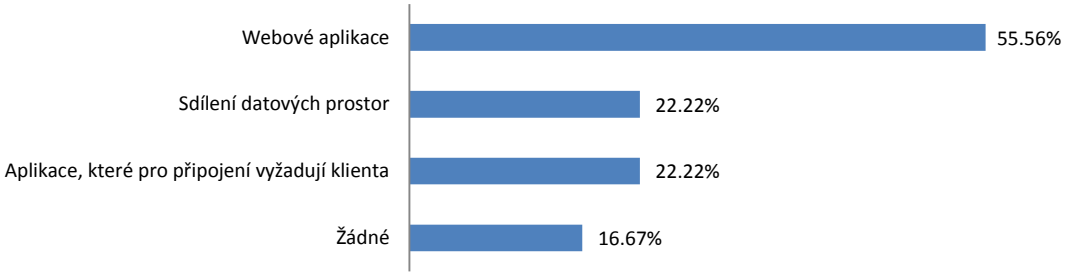


Graf 3-24: Mají uživatelé povinnost v pravidelných intervalech měnit svá hesla?

Zdroj: vlastní zpracování

Otázka č. 25: Jaké prostředky interní sítě mohou využívat externí partneři?

Občas bývá nutné poskytnout externím partnerům přístup do privátní sítě, což je náročné na zabezpečení, a proto je umožněn přístup pouze k některým prostředkům. Nejčastěji je povolen přístup k webovým aplikacím, které by však měly být psány s důrazem na jejich zabezpečení (např. proti SQL injection nebo krádež session).

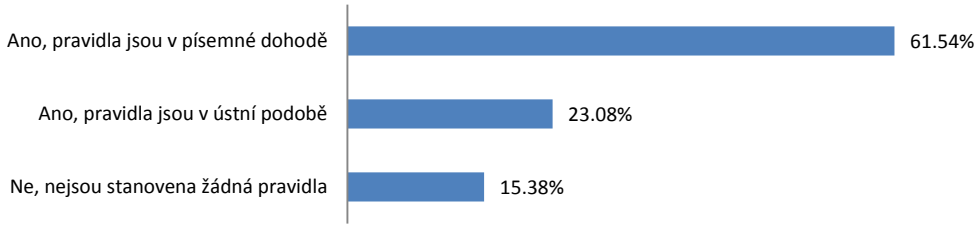


Graf 3-25: Jaké prostředky interní sítě mohou využívat externí partneři?

Zdroj: vlastní zpracování

Otázka č. 26: Je partner využívající systémy univerzity vázán bezpečnostními pravidly?

Přístup k systémům externími partnery by se měl řídit určitými pravidly, ta by měla být definována zejména v písemné podobě. Tímto lze lépe kontrolovat kompetence v rámci přístupu a vymezit zásady pro práci se systémem, kam má externí partner přístup.

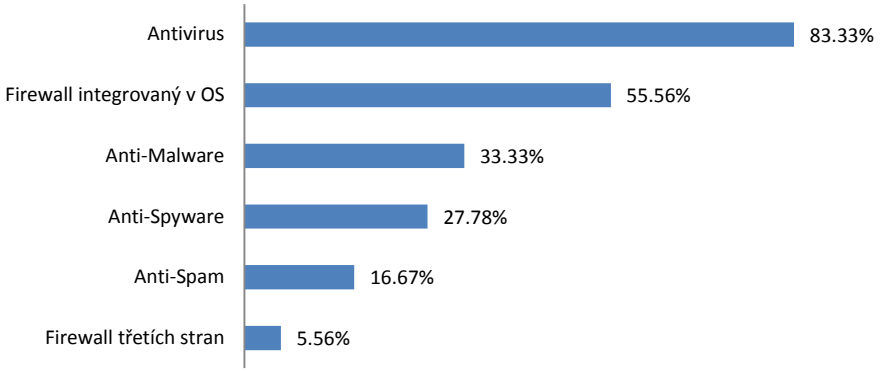


Graf 3-26: Je partner využívající systémy univerzity vázán bezpečnostními pravidly?

Zdroj: vlastní zpracování

Otázka č. 27: Které z následujících prostředků jsou nasazeny na pracovních stanicích pro zajištění jejich bezpečnosti?

Vysoké školy zajišťují bezpečnost počítačových stanic v jejich vlastnictví především s využitím antivirových řešení v kombinaci s použitím firewallu a v některých případech ještě doplněné o další typ bezpečnostního softwaru.

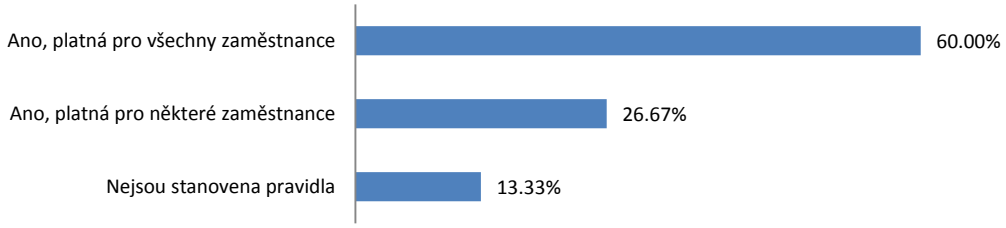


Graf 3-27: Které z následujících prostředků jsou nasazeny na pracovních stanicích pro zajištění jejich bezpečnosti?

Zdroj: vlastní zpracování

Otázka č. 28: Jsou stanovena pravidla pro zaměstnance v souvislosti s instalací programového vybavení na pracovních stanicích?

Pravidla pro instalaci počítačových programů přímo ovlivňují bezpečnost počítačových stanic. Více než polovina vysokých škol má stanovena pravidla týkající se instalace programového vybavení, která musí být dodržována všemi zaměstnanci univerzity.

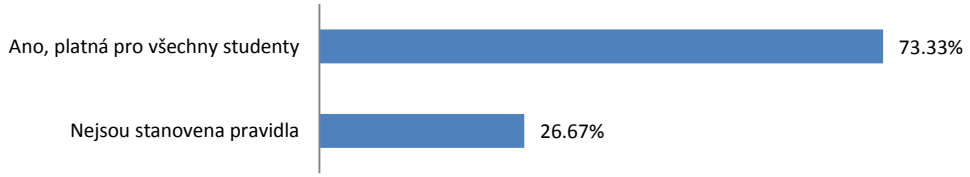


Graf 3-28: Jsou stanovena pravidla pro zaměstnance v souvislosti s instalací programového vybavení na pracovních stanicích?

Zdroj: vlastní zpracování

Otázka č. 29: Jsou stanovena pravidla pro studenty v souvislosti s instalací programového vybavení na pracovních stanicích?

Stejně jako pro zaměstnance, tak i pro studenty by měla být stanovena pravidla pro instalaci programového vybavení. Velice zvláštní však je, že většina univerzit má stanovena pravidla pro zaměstnance, tak v případě studentských oprávnění má taková pravidla menší část.



Graf 3-29: Jsou stanovena pravidla pro studenty v souvislosti s instalací programového vybavení na pracovních stanicích?

Zdroj: vlastní zpracování

4 VYHODNOCENÍ PRŮZKUMU

Vyhodnocení dotazníkového šetření je nezbytnou součástí, bez které by nebylo možné vyvodit závěry. Zkoumáním jednotlivých grafů lze vyvodit určité obecné závěry, ale nelze určit, jak si z hlediska bezpečnosti stojí jednotlivé školy. Pro ohodnocení bezpečnosti bylo použito bodové hodnocení organizační a síťové bezpečnosti, každé samostatně. Pro samotné hodnocení byl použit program Microsoft Excel.

4.1 Bodové hodnocení organizační bezpečnosti

Bodové ohodnocení proběhlo na základě odpovědí vybraných otázek, přičemž maximální počet bodů za jednotlivé otázky se lišil a byl stanoven na základě posouzení autora. Důvodem je, že určitá fakta mají různý stupeň vlivu na samotnou bezpečnost. Jelikož byla data dotazníku anonymizována, budou jednotlivé univerzity a vysoké školy značeny jako VŠ_1, VŠ_2, VŠ_3 atd. Hodnocení bude prezentováno ve formě tabulky.

Vybrané otázky, které budou použity pro hodnocení, budou dále uvedeny spolu s maximálním počtem bodů (každé otázce, případně skupině otázek je přiřazena jiná váha) a množstvím bodů podle typu odpovědi spolu s vysvětlením, proč bylo takto rozhodnuto. Některé otázky byly sloučeny, jelikož se zaměřují na podobnou oblast:

- Otázky zaměřené na zodpovědnost ohledně informační bezpečnosti byly sloučeny, přičemž maximální ohodnocení otázek dohromady je 3 body. Maximálního ohodnocení bylo dosaženo, pokud na univerzitě existuje zaměstnanec, který má informační bezpečnost jako hlavní pracovní náplň a existuje útvar, v jehož rámci je bezpečnost zakotvena. Bodové hodnocení se poté přímo úměrně snižuje, pokud je informační bezpečnost vedlejší pracovní náplní (případně taková osoba neexistuje) a pokud žádný útvar nemá zodpovědnost za informační bezpečnost.

- Nejenže je nutné, aby bezpečnost informací byla zajištěna technickými prostředky, ale také zaměstnanci by měli alespoň zběžně znát základní aspekty informační bezpečnosti. Pokud na univerzitě existuje program, který vzdělává zaměstnance v oblasti informační bezpečnosti, bylo dosaženo maximálního

počtu 1 bod. V případě, že takový program je hodnocen jako nefunkční, bylo dosaženo 0,5 bodu.

- Je důležité, aby informační bezpečnost byla definována v rámci nějakého dokumentu. Lze předpokládat, že čím delší tento dokument bude, tím více oblastí informační bezpečnosti dokáže pokrýt a bude tedy lépe sloužit. Zde byly rozlišeny 3 kategorie, rozsáhlý dokument za 3 body, středně dlouhý dokument za 2 body a stručný dokument za 1 bod. Navíc pokud tento dokument byl formálně přijat vedením univerzity, bylo toto ohodnoceno navíc 1 bodem. V úvahu byla brána také aktualizace dokumentu, pravidelná aktualizace 1 bodem, nepravidelná aktualizace 0,5 bodem. Bodový strop je zde tedy 5 bodů.

- Pokud je využíván nějaký mezinárodně uznávaný standard z oblasti informační bezpečnosti, lze předpokládat, že univerzita má určena aktiva, která je nutné chránit, rizika bezpečnosti informací jsou identifikována a řízena a jsou zavedena nezbytná bezpečnostní opatření. Pokud univerzita využívá nějakého standardu, je toto ohodnoceno maximálním počtem 4 bodů, pokud univerzita používá vlastních směrnic a standardů (nelze předpokládat, že vlastní standardy budou stejně kvalitní, jako ty mezinárodně uznávané), bylo dosaženo 2 bodů.

- Aktivity spojené s informační bezpečností je nutné také zabezpečit s finančního hlediska, proto pokud univerzita vynakládá nějaké finance na informační bezpečnost, bylo toto ohodnoceno 2 body.

Vysoká škola	Zodpovědnost za informační bezpečnost	Program vzdělávání	Dokument informační bezpečnosti	Bezpečnostní standardy	Vyhrazený rozpočet	Celkový počet bodů	Procentuální ohodnocení
VŠ_1	3	1	3,5	4	0	11,5	76,67%
VŠ_2	2	0	1	2	0	5	33,33%
VŠ_3	0	0	1	0	0	1	6,67%
VŠ_4	2	0	1,5	2	0	5,5	36,67%
VŠ_5	2	0	2,5	4	0	8,5	56,67%
VŠ_6	2	0,5	0	2	0	4,5	30,00%
VŠ_7	2	0	1	2	0	5	33,33%
VŠ_8	2	0	3	4	0	9	60,00%
VŠ_9	2	0	2,5	2	0	6,5	43,33%
VŠ_10	2	0	3,5	2	0	7,5	50,00%
VŠ_11	3	0	0	4	2	9	60,00%
VŠ_12	2	0,5	2,5	4	0	9	60,00%
VŠ_13	2	0	1	2	0	5	33,33%
VŠ_14	3	0,5	3,5	2	0	9	60,00%
VŠ_15	1	0	1,5	2	0	4,5	30,00%
VŠ_16	3	0,5	1,5	2	2	9	60,00%
VŠ_17	2	0	0	4	0	6	40,00%
VŠ_18	2	0	1	2	0	5	33,33%
Max	3	1	5	4	2	15	

Tab. 4-1: Hodnocení organizační bezpečnosti jednotlivých univerzit a vysokých škol

Zdroj: vlastní zpracování

Každé hodnocené univerzitě bylo na základě zjištěných bodů přiřazeno navíc procentuální vyjádření jejich hodnocení vzhledem k maximálně dosažitelnému počtu bodů. Závěrečné hodnocení se odvíjí od procentuálního vyjádření bodů, nad 75 % bylo hodnoceno jako velmi dobrá organizační bezpečnost, nad 50 % dobrá organizační bezpečnost, nad 25 % slabá organizační bezpečnost a pod 25 % se již v podstatě nedá hovořit o organizační bezpečnosti. Výsledky jsou prezentovány v tab. 4-1 a procentuální výsledky jsou barevně rozlišeny. V 8 případech z 18 bylo hodnocení jako alespoň dobré zabezpečení, v 1 případě lze konstatovat, že zabezpečení téměř neexistuje.

Pro porovnání je dále uvedena tabulka, která porovnává autorovo hodnocení s hodnocením samotných univerzit a vysokých škol. Jak je z následující tabulky patrné, tak pouze v 6 případech se autorovo hodnocení shodovalo s hodnocením univerzity. Proto lze předpokládat, že hodnocení univerzity není plně objektivní.

Vysoká škola	Hodnocení univerzity	Hodnocení autora	Vysoká škola	Hodnocení univerzity	Hodnocení autora
VŠ_1	výborná úroveň	Velmi dobré	**VŠ_10**	nízká úroveň	Dobré
VŠ_2	dobrá úroveň	Slabé	**VŠ_11**	nízká úroveň	Dobré
VŠ_3	dobrá úroveň	Žádné	**VŠ_12**	dobrá úroveň	Dobré
VŠ_4	dobrá úroveň	Slabé	**VŠ_13**	dobrá úroveň	Slabé
VŠ_5	dobrá úroveň	Dobré	**VŠ_14**	dobrá úroveň	Dobré
VŠ_6	dobrá úroveň	Slabé	**VŠ_15**	nízká úroveň	Slabé
VŠ_7	dobrá úroveň	Slabé	**VŠ_16**	dobrá úroveň	Dobré
VŠ_8	dobrá úroveň	Dobré	**VŠ_17**	dobrá úroveň	Slabé
VŠ_9	dobrá úroveň	Slabé	**VŠ_18**	dobrá úroveň	Slabé

Tab. 4-2: Rozdíl v hodnocení organizační bezpečnosti mezi autorem a univerzitami
Zdroj: vlastní zpracování

4.2 Bodové hodnocení technické bezpečnosti

Bodové hodnocení síťové bezpečnosti bylo provedeno podobným způsobem jako hodnocení organizační bezpečnosti. Zde však bylo třeba brát v úvahu, že ne všechny univerzity poskytují stejné možnosti studentům a zaměstnancům, proto celkový maximální počet bodů, který univerzita mohla získat, byl rozdílný. Pro hodnocení bylo využito těchto otázek a za jednotlivé odpovědi byl udělen následující počet bodů:

- Jednotný účet pro přihlášení do univerzitních systémů je výhodným bezpečnostním opatřením jak pro uživatele, tak pro univerzity samotné. Proto pokud univerzita umožňuje takové přihlašování do všech systémů, byl udělen maximální počet 2 bodů, pokud je využíván pouze do některých systémů, byl udělen 1 bod.

- Dalším hodnotícím kritériem bylo zabezpečení VPN připojení. V případě, že VPN připojení je zabezpečeno dvou-faktorově, tedy certifikátem i uživatelským jménem a heslem, bylo dosaženo maximálního počtu 2 bodů, pokud bylo zabezpečení provedeno jednou z předchozích možností, byl udělen 1 bod. V několika případech nebylo zjištěno, zda univerzita umožňuje VPN připojení, a proto těmto univerzitám byl snížen bodový strop, aby nebyly oproti ostatním znevýhodněny v hodnocení.

- Připojení zařízení UTP kabelem, které není vlastnictvím univerzity, je potřeba zabezpečit. Pokud je zabezpečení provedeno certifikátem, bylo toto hodnoceno 2 body, pokud na základě MAC adresy, tak 1 bodem, a pokud na základě pevné IP adresy, tak taktéž 1 bodem. Maximální počet bodů byl 3, pokud je zabezpečení provedeno na základě certifikátu a alespoň jedné z dalších možností. Některé univerzity nepovolují tento způsob připojení, a proto jejich maximální počet bodů byl snížen.

- Podle toho jakým způsobem probíhá autorizace a autentizace v rámci bezdrátové sítě byl při použití certifikátu a identity management serveru udělen maximální počet 3 bodů. Pokud byl použit jeden z výše uvedených způsobů, byly uděleny 2 body a pokud byla oprávnění přidělena na základě MAC adresy, byl udělen 1 bod.

- Šifrování bezdrátové komunikace je důležité, a proto při použití bezpečnější varianty WPA nebo WPA2 šifrování byl udělen maximální počet 2 bodů, pokud se jednalo o WEP zabezpečení, tak 1 bod.

- Přidělování oprávnění v rámci jednotlivých univerzitních systémů bylo hodnoceno maximálně 2 body, pokud je k řízení oprávnění použito seznamu, pokud se jedná o jiný způsob, byl přidělen 1 bod.

- Uživatelské heslo může být náchylné k prolomení anebo vyzrazení, proto je nutné mít nastaveny určité politiky ohledně zabezpečení hesel. Pokud je v systému nastavena minimální délka hesla alespoň 8 znaků, byly uděleny 2 body, pro kratší hesla byl udělen 1 bod. S tímto souvisí také změna hesla po určitém časovém úseku, při intervalu do jednoho roku byly uděleny 2 body a v případě delšího intervalu 1 bod. Maximálně tedy za toto kritérium mohly být uděleny 4 body.

- Některé univerzity umožňují externím partnerům přístup do svých systémů, proto by měly být pro tyto přístupy stanovena určitá pravidla. Pravidla stanovená v písemné podobě byla ohodnocena maximálním počtem 2 bodů a pravidla v ústní podobě 1 bodem.

- Důležité je, aby i samotné pracovní stanice byly určitým způsobem chráněny. Za používání firewallu (ať už šlo o zabudovaný firewall v operačním systému nebo firewall třetí strany) byl udělen 1 bod, za používání bezpečnostního softwaru (antiviru, anti-spywaru nebo anti-malwaru) byl udělen 1 bod a při používání antispamového filtru také 1 bod. Dohromady tedy mohly být uděleny maximálně 3 body.

- Není žádoucí, aby mohl kdokoliv instalovat na pracovních stanicích jakýkoliv software. Proto pokud jsou tato pravidla aplikována jak pro studenty, tak pro zaměstnance, byly uděleny 2 body, pokud se jednalo pouze o jedinou skupinu, byl udělen 1 bod.

Vysoká škola	Jednotný účet	VPN	Připojení UTP kabelem	Autentizace a autorizace na bezdrátové síti	Šifrování bezdrátové sítě	Udělování oprávnění
VŠ_1	0	nehodnoceno	0	0	0	0
VŠ_2	2	2	2	3	2	2
VŠ_3	0	1	1	2	2	2
VŠ_4	1	1	0	2	2	2
VŠ_5	2	2	3	2	2	2
VŠ_6	1	1	2	2	2	1
VŠ_7	2	1	2	2	2	1
VŠ_8	0	nehodnoceno	0	0	0	0
VŠ_9	1	2	1	2	2	2
VŠ_10	2	1	1	2	2	2
VŠ_11	2	1	nehodnoceno	1	2	1
VŠ_12	2	1	2	2	2	2
VŠ_13	2	1	nehodnoceno	2	2	2
VŠ_14	1	1	1	2	2	2
VŠ_15	1	1	0	2	2	2
VŠ_16	1	1	1	2	1	2
VŠ_17	2	1	1	2	2	2
VŠ_18	0	nehodnoceno	0	0	0	0
Max	2	2	3	3	2	2

Tab. 4-3: Hodnocení síťové bezpečnosti 1

Zdroj: vlastní zpracování

Vysoká škola	Politika hesel	Pravidla s externími partnery	Bezpečnost na stanicích	Pravidla ohledně instalace softwaru	Celkový počet bodů	Maximální počet bodů	Procentuální hodnocení
VŠ_1	nehodnoceno	nehodnoceno	0	0	Vyřazena		
VŠ_2	2	0	2	1	18	25	72,00%
VŠ_3	2	nehodnoceno	1	1	12	23	52,17%
VŠ_4	2	1	2	2	15	25	60,00%
VŠ_5	4	1	3	1	22	25	88,00%
VŠ_6	2	2	2	2	17	25	68,00%
VŠ_7	2	nehodnoceno	2	0	14	23	60,87%
VŠ_8	nehodnoceno	nehodnoceno	0	0	Vyřazena		
VŠ_9	2	2	1	2	17	25	68,00%
VŠ_10	4	1	2	2	19	25	76,00%
VŠ_11	4	2	3	1	17	22	77,27%
VŠ_12	4	2	2	2	21	25	84,00%
VŠ_13	3	2	2	2	18	22	81,82%
VŠ_14	2	2	2	2	17	25	68,00%
VŠ_15	nehodnoceno	2	2	2	14	21	66,67%
VŠ_16	2	2	1	2	15	25	60,00%
VŠ_17	4	nehodnoceno	2	2	18	23	78,26%
VŠ_18	nehodnoceno	nehodnoceno	0	0	Vyřazena		
Max	4	2	3	2		25	

Tab. 4-4: Hodnocení síťové bezpečnosti 2

Zdroj: vlastní zpracování

Vzhledem k tomu, že nebyly získány odpovědi z okruhu síťové bezpečnosti od 3 univerzit a vysokých škol, byly tyto ze závěrečného hodnocení vyřazeny (školy i výsledky jsou zaznamenány v tab. 4-3 a tab. 4-4), aby nebyly zkresleny výsledky. Pro hodnocení bylo použito stejných hodnotících intervalů jako v předchozím případě. Všech 15 škol získalo hodnocení alespoň dobré, z toho 6 škol získalo hodnocení velmi dobré. Lze konstatovat, že z hlediska síťové bezpečnosti si vysoké školy stojí celkem dobře a oproti organizační bezpečnosti jsou výsledky podstatně lepší.

Stejně jako v předchozím případě následuje tabulka s autorovým hodnocením a hodnocením samotných univerzit. Zde se hodnocení autora a hodnocení univerzit velmi neliší. Na druhou stranu v některých případech univerzitní hodnocení bylo horší než autorovo.

Vysoká škola	Hodnocení univerzity	Hodnocení autora	Vysoká škola	Hodnocení univerzity	Hodnocení autora
VŠ_1	výborná úroveň	Nehodnoceno	**VŠ_10**	nízká úroveň	Velmi dobré
VŠ_2	dobrá úroveň	Dobré	**VŠ_11**	nízká úroveň	Velmi dobré
VŠ_3	dobrá úroveň	Dobré	**VŠ_12**	dobrá úroveň	Velmi dobré
VŠ_4	dobrá úroveň	Dobré	**VŠ_13**	dobrá úroveň	Velmi dobré
VŠ_5	dobrá úroveň	Velmi dobré	**VŠ_14**	dobrá úroveň	Dobré
VŠ_6	dobrá úroveň	Dobré	**VŠ_15**	nízká úroveň	Dobré
VŠ_7	dobrá úroveň	Dobré	**VŠ_16**	dobrá úroveň	Dobré
VŠ_8	dobrá úroveň	Nehodnoceno	**VŠ_17**	dobrá úroveň	Velmi dobré
VŠ_9	dobrá úroveň	Dobré	**VŠ_18**	dobrá úroveň	Nehodnoceno

Tab. 4-5: Rozdíl v hodnocení síťové bezpečnosti mezi autorem a univerzitami

Zdroj: vlastní zpracování

Nakonec, aby bylo možné posoudit celkový stav informační bezpečnosti, byly použity procentuální výsledky obou hodnocení, ty byly zprůměrovány a znovu porovnány s hodnocením samotných univerzit. Z tohoto porovnání byly vyřazeny univerzity, které nebyly hodnoceny v rámci síťové bezpečnosti, v tab. 4-6 jsou pro přehlednost zvýrazněny (je u nich pouze uvedena hodnota za organizační bezpečnost).

Vysoká škola	Hodnocení univerzity	Hodnocení autora	%	Vysoká škola	Hodnocení univerzity	Hodnocení autora	%
VŠ_1	výborná úroveň	Nehodnoceno	76,67%	**VŠ_10**	nízká úroveň	Dobré	63%
VŠ_2	dobrá úroveň	Dobré	52,67%	**VŠ_11**	nízká úroveň	Dobré	68.64%
VŠ_3	dobrá úroveň	Slabé	29,42%	**VŠ_12**	dobrá úroveň	Dobré	72.00%
VŠ_4	dobrá úroveň	Slabé	48,33%	**VŠ_13**	dobrá úroveň	Dobré	57.58%
VŠ_5	dobrá úroveň	Dobré	72,33%	**VŠ_14**	dobrá úroveň	Dobré	64.00%
VŠ_6	dobrá úroveň	Slabé	49%	**VŠ_15**	nízká úroveň	Slabé	48.33%
VŠ_7	dobrá úroveň	Slabé	47,10%	**VŠ_16**	dobrá úroveň	Dobré	60.00%
VŠ_8	dobrá úroveň	Nehodnoceno	60%	**VŠ_17**	dobrá úroveň	Dobré	59.13%
VŠ_9	dobrá úroveň	Dobré	55,67%	**VŠ_18**	dobrá úroveň	Nehodnoceno	33.33%

Tab. 4-6: Celkové hodnocení organizační a síťové bezpečnosti

Zdroj: vlastní zpracování

Z výsledků bodových hodnocení bylo tedy určeno, jak si jednotlivé univerzity a vysoké školy stojí z pohledu informační bezpečnosti. Bližším zkoumáním jednotlivých otázek a okruhů otázek lze najít určité nedostatky. Například co velmi chybí v rámci organizační bezpečnosti je nějaký program vzdělávání zaměstnanců v oblasti informační bezpečnosti. Využívání mezinárodních, případně vlastních, standardů informační bezpečnosti je poměrně rozšířené napříč všemi univerzitami, avšak velmi málo z nich má definovanou

bezpečnostní politiku, která by byla schválena vedením univerzity. A pokud nějaký dokument stanovující bezpečnostní politiku existuje, pak se většinou jedná o velmi stručný text, který bývá zřídka aktualizovaný. Posledním bodem z hlediska organizační bezpečnosti bylo financování informační bezpečnosti, na kterou má vyhrazeny finance velmi malé množství univerzit. Z pohledu síťové bezpečnosti byly výsledky daleko lepší, ale určité nedostatky je možné zde také naleznout. Největším trnem v oku je zabezpečení sítě v souvislosti s používáním vlastních zařízení zaměstnanců a studentů připojených kabelem.

5 NÁVRH DOPORUČENÍ PRO ZVÝŠENÍ BEZPEČNOSTI NA VŠ

V předchozí kapitole, bylo provedeno hodnocení univerzit a vysokých škol a byly nalezeny nějaké nedostatky a mezery, které by mohly být příčinami nedostatečné informační bezpečnosti. Tato kapitola se bude snažit odpovědět na otázku, jak tyto nedostatky řešit. Obdobně jako v předchozích kapitolách budou návrhy rozděleny na ty, které se týkají organizační a ty, které se týkají síťové bezpečnosti.

5.1 Doporučení pro organizační bezpečnost

Jak již bylo zmíněno v závěru předchozí kapitoly, tak v rámci organizační bezpečnosti lze nalézt několik nedostatků, které je možné řešit.

Prvním takovým nedostatkem je to, že téměř na žádné univerzitě neexistuje program, který by vzdělával zaměstnance v oblasti informační bezpečnosti. Podle Doucka (2011, s. 58) existují zdroje, které uvádějí, že až 98 % všech bezpečnostních incidentů pochází zevnitř organizace, a že se většinou jedná o nedbalost zaměstnanců a neznalost problematiky informační bezpečnosti. Příkladem takového nesprávného chování je např. neodhlášení se nebo neuzamčení počítače při odchodu na přestávku nebo nepovolené stažení dat na vlastní paměťové médium. Tyto problémy lze řešit právě zavedením nějakého výchovného a školícího programu. Jako nejjednodušší a pravděpodobně i nejlevnější varianta se jeví vytvoření e-learningového kurzu s výstupním testem. Výhodou je, že jakmile je takový kurz vytvořen, může být zaveden v rámci informačního systému a v podstatě není třeba, aby informační bezpečnost školil lektor. Vhodné je, aby takovým kurzem prošel každý zaměstnanec, který pracuje s IS/ICT zdroji (a to poté co je kurz vytvořen anebo brzy po prvním nástupu do zaměstnání), a tento kurz se opakoval po uplynutí určité doby, např. každé 2 roky. Další předností e-learningového kurzu je, že je možné jej pořád opakovat a při zjištění nějakých nedostatků je snadné jej upravit. Druhou možností je vytvořit klasické školení zaměstnanců s lektorem, zde však bude vyšší organizační i finanční náročnost.

Dalším zjištěným nedostatkem bylo nepřítomnost formalizovaného dokumentu bezpečnostní politiky. V takovém dokumentu se nejčastěji nachází, jak se zachovat a jak řešit určité nestandardní situace a bezpečnostní incidenty, jaká aktiva se mají chránit. Je pravda, že bezpečnostní politika nemusí být velmi rozsáhlý dokument, ale musí být schopna zastřešit široké spektrum oblastí bezpečnosti. To vše je důvodem, proč by bezpečnostní politika měla

být v písemné podobě. Samozřejmě je důležité, aby byla dodržována a všem zainteresovaným známá. Jediným doporučením tedy je, aby takový dokument byl vytvořen, což by nemuselo být až tak náročné, jelikož univerzity většinou disponují zaměstnanci, kteří se alespoň částečně zabývají informační bezpečností. Také je možné zavést takový dokument s pomocí externího partnera či společnosti, ale šlo by o finančně náročnější řešení.

Posledním bodem pro doporučení vzhledem k organizační bezpečnosti je celkové financování informační bezpečnosti. Pouze 2 univerzity z celkových 18 mají pro tuto oblast vyhrazen rozpočet, i když ne samostatný, ale je součástí rozpočtu jiného útvaru. Avšak řízení rizik bez finančních prostředků není možné, a proto by nějaké finance na tuto oblast vyčleněny být měly (předpokládá se, že školy již nějakým softwarem a hardwarem řešícím bezpečnost disponují, ale tento je také třeba obnovovat). Nehledě na to, že v případě závažnějšího incidentu se odstranění jeho následků oproti prevenci může výrazně prodražit.

5.2 Doporučení ohledně síťové bezpečnosti

I přestože hodnocení síťové bezpečnosti dopadlo mezi univerzitami mnohem lépe, tak i zde lze nalézt příležitosti pro její zdokonalení.

Jako nejslabší místo síťové bezpečnosti se jeví používání zařízení studentů a zaměstnanců, které se do interní sítě připojují pomocí UTP kabelů. Ve většině případů je bezpečnost zajišťována pomocí seznamu MAC adres koncových zařízení. Toto bezpečnostní opatření však má několik nedostatků, za prvé MAC adresa je sice unikátní údaj každé síťové karty, který se nepřenáší po síti, ale stále je zjistitelný a za druhé existuje mnoho softwarových způsobů jak zajistit, aby zařízení navenek vypadalo, že má jinou MAC adresu než ve skutečnosti. V tomto ohledu by si univerzity měly vzít příklad z těch, které pro zabezpečení a ověření používají vygenerované certifikáty.

Dalším nedostatkem, i když je přítomen pouze u jediné univerzity, je používání WEP zabezpečení bezdrátové sítě. Toto zabezpečení bylo prolomeno již před více než 10 lety a existuje mnoho softwarových nástrojů, které umožňují např. odposlouchávání komunikace. Navíc stálý trend růstu množství používaných mobilních zařízení schopných se připojit k bezdrátové síti, zvyšuje pravděpodobnost hrozby právě odposlouchávání, případně také MITM útoku. A přitom není technologicky náročné využívat mnohem spolehlivějšího WPA2 zabezpečení.

Posledním závažnějším nedostatkem je, že ne vždy jsou aplikována pravidla pro instalaci softwaru na pracovních stanicích. To by mělo být pravidlem, jelikož vlastní software může být bezpečnostní hrozbou, a to zejména v případě pokud se jedná o jeho nelegální kopie. Samozřejmě je pochopitelné, že tento zákaz nemusí platit pro všechny zaměstnance, ale měl by vždy platit pro studenty, což v několika případech není zavedeno. Krom toho se také jedná o jedno z těch méně náročnějších opatření.

6 ZÁVĚR

Není tomu tak dávno, kdy mobilní technologie zvládaly pouze základní funkce telefonování a posílání textových zpráv. Velkou revolucí bylo, když mobilní telefony získaly barevné displeje a poté i poměrně slabé fotoaparáty. Ale co přišlo poté, se dá nazvat revolucí. Veškeré přístroje dnes patřící do rodiny moderních mobilních zařízení, chytré telefony, tablety i phablety se staly velmi výkonnými a mnohdy dokáží konkurovat notebookům a desktopovým starých několik málo let. Jejich obliba roste mezi běžnými uživateli a množství lidí, kteří vlastní takový přístroj je stále větší. A s tím jak oblíbenější a výkonnější jsou, tím více si také získávají na oblíbenosti ve firemní sféře, kde se stávají nedocenitelnými pomocníky a prostředkem pro zefektivnění pracovní činnosti a úsporu času. Není problém se pomocí nich připojit odkudkoliv k internetu, vytvářet kvalitní fotografie a videa, nechat se navigovat v rámci systému GPS a mnoho dalšího. Ale veškeré tyto přednosti a užitečné pomůcky na jednu stranu pomáhají a na druhou stranu jsou zdrojem mnoha problémů.

A právě problémům, tedy hrozbám spojeným s používáním mobilních technologií, zejména v rámci organizací, se věnovala první kapitola. Jsou zde popsány jednotlivé hrozby, co představují, jak se projevují, co je jejich podstatou a příčinou a také jaké mohou mít konečné dopady a důsledky nejen na samotného uživatele, ale i organizaci a její aktiva. Možnostem jak se těmto hrozbám vyhýbat anebo snižovat jejich dopad byl poskytnut prostor ve zbytku kapitoly. Byly uvedeny a charakterizovány přístupy a nástroje zabývající se problematikou podnikové mobility. Jmenovat lze třeba mobile device management, který je nejstarší z celého souboru zaměřeného na správu podnikové mobility a bezpečnost uživatelů, organizací a jejich aktiv. Bylo také objasněno to, že ne každá organizace musí nutně využívat celou širokou paletu těchto nástrojů, ale že lze využít pouze určitou podmnožinu z nich podle potřeby. Z toho vyplynulo, že nástroje správy podnikové mobility lze mezi ostatní informační systémy nasadit mnoha různými způsoby a řešit jimi různé potřeby uživatelů a různé potřeby organizací. Nejdůležitější však je, že je potřeba nalézt vybalancovaný přístup mezi jednotlivými možnostmi tak, aby řešení ve výsledku podporovalo zaměstnance a ne je omezovalo.

Zbytek diplomové práce pak byl soustředěn na organizační a síťovou bezpečnost v rámci českých vysokých škol a univerzit. Pomocí dotazníkového šetření byly zjištěny základní fakta o zapojených univerzitách a informace o tom, jakým způsobem řeší problematiku informační bezpečnosti. Zhodnocením jednotlivých otázek bylo poté zjištěno,

že síťová bezpečnost je na tom celkově lépe než organizační. Byly identifikovány největší nedostatky z obou oblastí, které by mohly mít nezanedbatelný vliv na bezpečnost. Nakonec bylo navrženo několik možností a doporučení, které mají za cíl celkově zlepšit informační bezpečnost na vysokých školách a univerzitách v České republice.

7 SEZNAM POUŽITÉ LITERATURY

Alcatel-Luscent. 2015. *Motive Security Labs malware report – H2 2014* [online]. [cit. 2015-04-10]. Dostupné z: https://resources.alcatel-lucent.com/asset/184652

DOUCEK, Petr. 2011. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2. vyd. Praha: Professional Publishing, 286 s. ISBN 978-80-7431-050-8.

ENISA. 2010. *Smartphone security: Information security risks, opportunities and recommendations for users* [online]. [cit. 2015-04-07]. Dostupné z: https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

Gartner, Inc.. 2015. *Magic Quadrant for Enterprise Mobility Management Suites* [online]. [cit. 2015-06-27]. Dostupné z: http://www.gartner.com/technology/reprints.do?id=1-2HF4VDW&ct=150608&st=sb

ISO/IEC 18004:2015. 2015. *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification*. Geneva: International Organization for Standardization. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:18004:ed-3:v1:en

ISO/IEC 27000:2014. 2014. *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*. Geneva: International Organization for Standardization, 31 s. Dostupné z: http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip

MADDEN, Jack. 2014. *Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD*. San Francisco: Jack Madden, 187 p. ISBN 978-9896506-1-8.

MATOUŠKOVÁ, Ingrid a Roman RAK. 2013. *Bezpečnost firmy a podnikání*. Praha: BIVŠ, a.s., 262 s. ISBN 978-80-7265-228-0.

Microsoft Corp.. 2009. *Device Management with Mobile Device Manager* [online]. [cit. 2015-05-25]. Dostupné z: https://technet.microsoft.com/en-us/library/dd252758.aspx

NIST SP 800-124. 2013. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Rev 1. Gaithersburg: National Institute of Standards and Technology, 20 p.

ONDRÁK, Viktor a Petr SEDLÁK. 2013. *Problematika ISMS v manažerské informatice*. Brno: CERM, 377 s. ISBN 978-80-7204-872-4.

RHODES-OUSLEY, Mark. 2012. *Information Security the Complete Reference*. 2nd ed. New York: McGraw Hill, 896 p. ISBN 978-007-1784-351.

STERK, Peter. 2014. *Enterprise Mobility Management Smackdown* [online]. De Meern: PQR B.V. [cit. 2015-05-22]. Dostupné z: http://dynamixgroup.com/sites/default/files/field/image/whitepaper_emm_smackdown.compressed_0.pdf

Symantec. ©2012. *The Symantec Smartphone Honey Stick Project* [online]. [cit. 2015-04-08]. Dostupné z: http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf

Monografie:

DOUCEK, Petr. 2011. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2. vyd. Praha: Professional Publishing, 286 s. ISBN 978-80-7431-050-8.

MADDEN, Jack. 2014. *Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD*. San Francisco: Jack Madden, 187 p. ISBN 978-9896506-1-8.

MATOUŠKOVÁ, Ingrid a Roman RAK. 2013. *Bezpečnost firmy a podnikání*. Praha: BIVŠ, a.s., 262 s. ISBN 978-80-7265-228-0.

ONDRÁK, Viktor a Petr SEDLÁK. 2013. *Problematika ISMS v manažerské informatice*. Brno: CERM, 377 s. ISBN 978-80-7204-872-4.

RHODES-OUSLEY, Mark. 2012. *Information Security the Complete Reference*. 2nd ed. New York: McGraw Hill, 896 p. ISBN 978-007-1784-351.

STERK, Peter. 2014. *Enterprise Mobility Management Smackdown* [online]. De Meern: PQR B.V. [cit. 2015-05-22]. Dostupné z: http://dynamixgroup.com/sites/default/files/field/image/whitepaper_emm_smackdown.compressed_0.pdf

Elektronické zdroje:

Alcatel-Luscent. 2015. *Motive Security Labs malware report – H2 2014* [online]. [cit. 2015-04-10]. Dostupné z: https://resources.alcatel-lucent.com/asset/184652

ENISA. 2010. *Smartphone security: Information security risks, opportunities and recommendations for users* [online]. [cit. 2015-04-07]. Dostupné z: https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users/at_download/fullReport

Gartner, Inc.. 2015. *Magic Quadrant for Enterprise Mobility Management Suites* [online]. [cit. 2015-06-27]. Dostupné z: http://www.gartner.com/technology/reprints.do?id=1-2HF4VDW&ct=150608&st=sb

ISO/IEC 18004:2015. 2015. *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification*. Geneva: International

Organization for Standardization. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:18004:ed-3:v1:en

ISO/IEC 27000:2014. 2014. *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary*. Geneva: International Organization for Standardization, 31 s. Dostupné z: http://standards.iso.org/ittf/PubliclyAvailableStandards/c063411_ISO_IEC_27000_2014.zip

Microsoft Corp.. 2009. *Device Management with Mobile Device Manager* [online]. [cit. 2015-05-25]. Dostupné z: https://technet.microsoft.com/en-us/library/dd252758.aspx

NIST SP 800-124. 2013. *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Rev 1. Gaithersburg: National Institute of Standards and Technology, 20 p. Dostupné z: http://csrc.nist.gov/publications/drafts/800-124r1/draft_sp800-124-rev1.pdf

Symantec. ©2012. *The Symantec Smartphone Honey Stick Project* [online]. [cit. 2015-04-08]. Dostupné z: http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf

8 SEZNAM ZKRATEK A POJMŮ

BYOD	Bring Your Own Device, dones si své zařízení, přístup využívání vlastních zařízení v zaměstnání
COPE	Corporate Owned, Personally Enabled, přístup využívání firemních zařízení i pro osobní účely
EMM	Enterprise Mobility Management, Správa podnikové mobility
ENISA	European Network and Information Security Agency, Evropská agentura pro bezpečnost sítí a informací
IMEI	International Mobile Equipment Identity, unikátní číslo mobilního telefonu
MAC	Media Access Control, MAC adresa je unikátní číselný identifikátor síťové karty
MAM	Mobile Application Management, Správa mobilních aplikací
MCM	Mobile Content Management, Správa mobilního obsahu
MDM	Mobile Device Management, Správa mobilních zařízení
MEM	Mobile Email/Expense Management, Správa mobilních výdajů/emailů
MIM	Mobile Information Management, Správa mobilních informací
MITM	Man in the middle, člověk uprostřed – typ útoku, kdy se útočník snaží odposlouchávat komunikaci
NFC	Near field communication, technologie komunikace mezi dvěma zařízeními na velmi malou vzdálenost
NIST	National Institute of Standards and Technology, Národní institut standardů a technologie

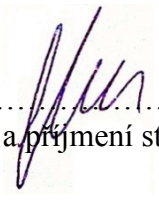
OMA DM	Open Mobile Alliance Device Management, protokol používaný v rámci MDM komunikace
OS	Operating system, operační systém
OTA	Over the air, vzduchem – reference na vzdálenou správu
QR	Quick response, označení kódů rychlé reakce – QR kódů
VPN	Virtual private network, virtuální privátní síť
WEP	Wired Equivalent Privacy, soukromí ekvivalentní drátovým sítím – technologie zabezpečení bezdrátové komunikace
Wi-Fi	Wireless fidelity, bezdrátová věrnost, technologie bezdrátové komunikace
WPA/WPA2	Wi-Fi Protected Access, chráněný přístup k Wi-Fi – technologie zabezpečení bezdrátové komunikace

Prohlášení o využití výsledků diplomové (bakalářské) práce

Prohlašuji, že

- jsem byl(a) seznámen(a) s tím, že na mou diplomovou (bakalářskou) práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou (bakalářskou) práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová (bakalářská) práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové (bakalářské) práce. Souhlasím s tím, že bibliografické údaje o diplomové (bakalářské) práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou (bakalářskou) práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne ……



……
jméno a příjmení studenta

9 SEZNAM PŘÍLOH

Příloha č. 1 Data z dotazníkového šetření

1 PŘÍLOHA Č. 1 DATA Z DOTAZNÍKOVÉHO ŠETŘENÍ

Username	Název Vaší instituce?	Kolik zaměstnanců má Vaše vysoká škola/univerzita?	Kolik studentů všech typů studia na Vaší vysoké škole/univerzitě studuje?	Jaké obory studia nabízíte na Vaší vysoké škole/univerzitě?
		2944	23528	Humanitní i technické
		1640	11207	Humanitní i technické
		2000	7800	Humanitní i technické
		3000	22000	Humanitní i technické
		2500	15000	Humanitní i technické
		850	10500	Humanitní i technické
		950	3500	Technické
		656	7579	Humanitní i technické
			16000	Humanitní i technické
		500	11000	Humanitní i technické
		2500	19000	Technické
		1150	9780	Humanitní i technické
		1000	11000	Humanitní i technické
		2562	12665	Humanitní i technické
		900	10500	Humanitní i technické
		cca 1300	cca 18000	Humanitní i technické
		cca 4000	21000	Technické
		2500	25000	Humanitní i technické

Jakého typu z pohledu zřizovatele je Vaše vysoká škola/univerzita?	Jaká je Vaše pozice v rámci vysoké školy/univerzity?	Věnuje se některý pracovník Vaší organizace informační bezpečnosti jako hlavní pracovní náplni?	Kdo je na Vaší vysoké škole/univerzitě zodpovědný za řešení informační bezpečnosti?
Státní/veřejná	Ředitel IS/IT	ano	Manažer - vedoucí oddělení
Státní/veřejná	Vedoucí oddělení IS/IT	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Vedoucí oddělení IS/IT	ne	Nikdo
Státní/veřejná	Rektor/děkan	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Vedoucí oddělení IS/IT	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Ředitel IS/IT	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Specialista IS/IT	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Ředitel IS/IT	ne	Člen nejvyššího vedení
Státní/veřejná	Rektor/děkan	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Specialista IS/IT	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Ředitel IS/IT	ano	Specialista - nemanažerská pozice
Státní/veřejná	Ředitel IS/IT	ne	Manažer - vedoucí oddělení
Státní/veřejná	Ředitel IS/IT	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Specialista IS/IT	ano	Specialista - nemanažerská pozice
Státní/veřejná	Ředitel IS/IT	ne	Zodpovědnost mezi více lidí
Státní/veřejná	Ředitel IS/IT	ano	Člen nejvyššího vedení
Státní/veřejná	Ředitel IS/IT	ne	Manažer - vedoucí oddělení
Státní/veřejná	Ředitel IS/IT	ne	Manažer - vedoucí oddělení

Který útvar je zodpovědný za informační bezpečnost na Vaší vysoké škole/univerzitě?	Existuje na Vaší vysoké škole/univerzitě funkční program zvyšování povědomí zaměstnanců v oblasti informační bezpečnosti (nikoliv BOZP)?	Jak hodnotíte vlastní úroveň řešení bezpečnosti?	Vyberte prosím 3 faktory, kte	
			hrozba útoku	výsledky provedeného auditu/doporučení auditorů
Útvar IS/IT	ano	výborná úroveň	ano	ne
Útvar IS/IT	ne	dobrá úroveň	ano	ne
Žádný útvar	ne	dobrá úroveň	ne	ne
Útvar IS/IT	ne	dobrá úroveň	ano	ano
jiný útvar	ne	dobrá úroveň	ano	ne
Útvar IS/IT	ano, ale spíše nefunkční	dobrá úroveň	ano	ano
Útvar IS/IT	ne	dobrá úroveň	ano	ano
Útvar IS/IT	ne	dobrá úroveň	ano	ne
Útvar IS/IT	ne	dobrá úroveň	ano	ne
Útvar IS/IT	ne	nízká úroveň	ano	ne
Útvar IS/IT	ne	nízká úroveň	ano	ano
Útvar IS/IT	ano, ale spíše nefunkční	dobrá úroveň	ano	ne
Útvar IS/IT	ne	dobrá úroveň	ano	ne
Útvar IS/IT	ano, ale spíše nefunkční	dobrá úroveň	ne	ano
Žádný útvar	ne	nízká úroveň	ano	ne
Útvar IS/IT	ano, ale spíše nefunkční	dobrá úroveň	ne	ano
Útvar IS/IT	ne	dobrá úroveň	ne	ne
Útvar IS/IT	ne	dobrá úroveň	ano	ne

ré mají největší vliv na prosazování informační bezpečnosti na Vaší vysoké				Má Vaše vysoká škola/univerzita ve formě dokumentu formálně definovanou a nejvyšším vedením přijatou bezpečnostní politiku?
aplikace zákona o ochraně osobních údajů	tlak/požadavky ze strany vrcholového vedení	řešení informační bezpečnosti u srovnatelných organizací	hrozba finančních sankcí	
ne	ano	ano	ne	ano
ne	ano	ne	ano	ne
ano	ne	ano	ne	ne
ne	ne	ano	ne	ne
ne	ano	ne	ano	ano
ano	ne	ne	ne	ne
ne	ne	ano	ne	ne
ano	ne	ano	ne	ne
ne	ne	ano	ne	ne
ne	ne	ano	ano	ano
ano	ne	ne	ne	ne
ano	ne	ne	ano	ne
ano	ne	ne	ano	ne
ano	ne	ano	ano	ano
ano	ne	ne	ano	ne
ano	ano	ne	ne	ne
ano	ano	ano	ne	ne
ano	ne	ne	ano	ne

Jaký je rozsah dokumentu bezpečnostní politiky?	Jak často dochází k aktualizaci dokumentu bezpečnostní politiky?	Jaké mezinárodní standardy v oblasti informační bezpečnost			
		vlastní interní standardy a směrnice	ISO/IEC 17799/BS 7799 (britský standard), ISO 27000	ITIL	ISO/IEC TR 13335
střední - cca do 20 stran	nepravidelně, podle potřeby	ano	ne	ano	ne
stručný - cca do 3 stran	není aktualizován	ano	ne	ne	ne
stručný - cca do 3 stran	není aktualizován	ne	ne	ne	ne
stručný - cca do 3 stran	nepravidelně, podle potřeby	ano	ne	ne	ne
stručný - cca do 3 stran	nepravidelně, podle potřeby	ano	ano	ano	ne
null	null	ano	ne	ne	ne
stručný - cca do 3 stran	není aktualizován	ano	ne	ne	ne
rozsáhlý - několik desítek stran	není aktualizován	ne	ne	ne	ne
střední - cca do 20 stran	nepravidelně, podle potřeby	ano	ne	ne	ne
střední - cca do 20 stran	nepravidelně, podle potřeby	ano	ne	ne	ne
null	null	ne	ano	ne	ne
střední - cca do 20 stran	nepravidelně, podle potřeby	ano	ano	ne	ne
stručný - cca do 3 stran	není aktualizován	ano	ne	ne	ne
střední - cca do 20 stran	nepravidelně, podle potřeby	ano	ne	ne	ne
stručný - cca do 3 stran	nepravidelně, podle potřeby	ano	ne	ne	ne
stručný - cca do 3 stran	nepravidelně, podle potřeby	ano	ne	ne	ne
null	null	ne	ano	ne	ne
stručný - cca do 3 stran	není aktualizován	ano	ne	ne	ne

ti a/nebo IT governance jsou v rámci Vaší vysoké školy/univerzity					Má Vaše vysoká škola/univerzita vyčleněný samostatný rozpočet pro financování informační bezpečnosti?
COBIT	jiný standard	standardy a nařízení Evropské unie pro oblast bezpečnosti IS	standardy a publikace NIST pro oblast bezpečnosti IS/IT	standard německého BSI	
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ano	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ano	ne	ne	ne	ne	ano, v rámci rozpočtu jiného útvaru
ano	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ano, v rámci rozpočtu jiného útvaru
ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne

Jaké části IS/IT outsourcujete (alespoň částečně) na Vaší vysoké škole/univerzitě								
správa LAN/WAN	vývoj aplikací	správa firewallu	internetové připojení	provoz/údržba IS/IT	správa databází	Helpdesk	finanční/účetní systém/informační systém podporující klíčové procesy školy (udělování zkoušek, zápočtů, studentská agenda)	bezpečnostní monitoring
ne	ne	ne	ne	ne	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne	ne	ano	ne
ne	ne	ne	ne	ne	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne	ne	ano	ne
ne	ne	ne	ne	ne	ne	ne	ne	ne
ne	ne	ne	ne	ne	ne	ne	ne	ne
ne	ano	ne	ne	ne	ano	ne	ano	ne
ne	ne	ne	ne	ne	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne	ne	ne	ne
ano	ne	ne	ne	ne	ne	ne	ano	ne
ne	ne	ne	ne	ne	ne	ne	ne	ne
ano	ano	ne	ne	ne	ano	ne	ne	ne
ne	ne	ne	ne	ne	ne	ne	ne	ne
ne	ano	ne	ne	ne	ano	ne	ano	ne
ne	ano	ne	ne	ne	ano	ne	ne	ne
ne	ano	ne	ano	ne	ano	ne	ano	ne
ne	ano	ne	ne	ne	ne	ne	ano	ne
ne	ne	ne	ne	ne	ne	ne	ne	ne

		Jaký využíváte systém řízení uživatelských účtů?
žádné	**jiná část. Prosím uveďte, o jakou část se jedná:**	
ne	ne	null
ne	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ano	ne	null
ne	ne	Jednotný účet pro přihlášení je zaveden, ale nepoužívá se u všech systémů
ano	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ano	ne	Jednotný účet není zaveden, ale využíváme autentizační server (např. LDAP nebo AD)
ne	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ne	ne	null
ne	ne	Jednotný účet pro přihlášení je zaveden, ale nepoužívá se u všech systémů
ne	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ano	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ne	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ano	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ne	ne	Jednotný účet pro přihlášení je zaveden, ale nepoužívá se u všech systémů
ne	ne	Jednotný účet pro přihlášení je zaveden, ale nepoužívá se u všech systémů
ne	ne	Jednotný účet pro přihlášení je zaveden, ale nepoužívá se u všech systémů
ne	ne	Do všech systémů (např. IS, pošta, služby, ...) je využíván jednotný účet pro přihlášení (např. LDAP)
ne	ne	null

Využívá organizace vzdálené uživatelské VPN přístupy?	Jakým způsobem jsou uživatelé při přístupu přes VPN ověřování?			Způsob přidělování oprávn
	Certifikáten	Pomocí uživatelského jména a hesla	Jiným způsobem. Prosím, uveďte	Přidělování přístupu na základě MAC adresy
null	ne	ne	ne	ne
ano	ano	ano	ne	ano
ano	ne	ano	ne	ano
ano	ne	ano	ne	ne
ano	ano	ano	ne	ano
ano	ano	ne	ne	ne
ano	ne	ano	ne	ne
null	ne	ne	ne	ne
ano	ano	ano	ne	ano
ano	ne	ano	ne	ano
ano	ne	ano	ne	ano
ano	ne	ano	ne	ne
ano	ne	ano	ne	ne
ano	ne	ano	ne	ano
ano	ne	ano	ne	ne
ano	ne	ano	ne	ano
ano	ne	ano	ne	ano
null	ne	ne	ne	ne

ění pro přístup k lokální síti s vlastním zařízením (připojení zařízení pomocí kabelu).			Způsob přidělování oprávnění pro přís	
Ověřování s využitím vygenerovaného certifikátu	Ověřování na základě pevně stanovené IP adresy	Přístup s vlastním zařízením není umožněn	Přidělování přístupu na základě MAC adresy	Ověřování s využitím vygenerovaného certifikátu
ne	ne	ne	ne	ne
ne	ano	ne	ne	ano
ne	ne	ne	ne	ne
ne	ne	ne	ne	ne
ano	ne	ne	ne	ne
ano	ne	ne	ne	ne
ano	ne	ne	ne	ne
ne	ne	ne	ne	ne
ne	ne	ne	ne	ne
ne	ne	ne	ne	ne
ne	ne	ano	ano	ne
ano	ne	ne	ne	ne
ne	ne	ano	ne	ne
ne	ne	ne	ne	ne
ne	ne	ne	ne	ne
ne	ne	ne	ne	ne
ne	ne	ne	ne	ne
ne	ne	ne	ne	ne

up k Wi-Fi síti s vlastním zařízením.		Jaký typ šifrování komunikace využíváte ve Wi-Fi síti?				
IDM Server (např. Radius server)	Přístup s vlastním zařízením není umožněn	WEP	WEP2	WPA	WPA2	Žádné šifrování
ne	ne	ne	ne	ne	ne	ne
ano	ne	ne	ne	ano	ano	ne
ano	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ano	ano	ne
ano	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ne	ano	ne
ne	ne	ne	ne	ne	ne	ne
ano	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ne	ano	ne
ne	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ne	ano	ne
ano	ne	ne	ne	ano	ano	ne
ano	ne	ano	ne	ne	ne	ne
ano	ne	ne	ne	ne	ano	ne
ne	ne	ne	ne	ne	ne	ne

Přidělování práv k uživatelským účtům	Je stanovena minimální délka hesla pro přístup k uživatelskému účtu?	Mají uživatelé povinnost v pravidelných intervalech měnit svá hesla?
null	null	null
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ne, hesla není nutné měnit
Na základě seznamu oprávnění pro danou pozici	ano (6 znaků)	Ano, v intervalu delším než 1 rok
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ne, hesla není nutné měnit
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ano, nejpozději každých 6 měsíců
Ad-hoc	ano (8 znaků)	Ne, hesla není nutné měnit
Ad-hoc	ano (8 znaků)	Ne, hesla není nutné měnit
null	null	null
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ne, hesla není nutné měnit
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ano, nejpozději každých 6 měsíců
Všem uživatelům jsou přiřazena stejná práva	ano (9 znaků)	Ano, nejpozději po jednom roce
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ano, nejpozději každých 6 měsíců
Na základě seznamu oprávnění pro danou pozici	ano (6 znaků)	Ano, nejpozději po jednom roce
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ne, hesla není nutné měnit
Na základě seznamu oprávnění pro danou pozici	null	null
Na základě seznamu oprávnění pro danou pozici	ano (8 znaků)	Ne, hesla není nutné měnit
Na základě seznamu oprávnění pro danou pozici	ano (8 kombinace druhÃÂ¯ z	Ano, nejpozději po jednom roce
null	null	null

Odebrání uživatelských účtů studentům:
null
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
null
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
Při události - standardizované procedury (např. ukončení studia; nezískání dostatečného počtu kreditů ke stanovenému datu; nedostavení se na zápis)
null

Odebrání uživatelských účtů zaměstnancům:
null
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
null
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
Při události - standardizované procedury (např. ukončení pracovního poměru; změna pracovní pozice zaměstnance, s níž souvisí zrušení účtů, které již dále pro práci r
null

Jaké prostředky interní sítě mohou využívat externí partneři?					Je partner využívající systémy univerzity vázán bezpečnostními pravidly?	Kt
Webové aplikace	Aplikace, které pro připojení vyžadují klienta	Sdílení datových prostor	Žádné	Jiné		Firewall integrovaný v OS
ne	ne	ne	ne	ne	null	ne
ano	ne	ne	ne	ne	Ne, nejsou stanovena žádná pravidla	ano
ne	ne	ne	ano	ne	null	ne
ano	ne	ne	ne	ne	Ano, pravidla jsou v ústní podobě	ano
ano	ano	ano	ne	ne	Ano, pravidla jsou v ústní podobě	ne
ne	ne	ne	ne	dle žádosti	Ano, pravidla jsou v písemné dohodě	ano
ne	ne	ne	ano	ne	Ne, nejsou stanovena žádná pravidla	ano
ne	ne	ne	ne	ne	null	ne
ano	ne	ne	ne	ne	Ano, pravidla jsou v písemné dohodě	ne
ano	ano	ne	ne	ne	Ano, pravidla jsou v ústní podobě	ano
ano	ne	ano	ne		Ano, pravidla jsou v písemné dohodě	ano
ano	ne	ne	ne	ne	Ano, pravidla jsou v písemné dohodě	ano
ne	ne	ne	ano	ne	Ano, pravidla jsou v písemné dohodě	ano
ano	ano	ano	ne	ne	Ano, pravidla jsou v písemné dohodě	ano
ano	ano	ne	ne	ne	Ano, pravidla jsou v písemné dohodě	ano
ano	ne	ano	ne	ne	Ano, pravidla jsou v písemné dohodě	ne
ne	ne	ne	ne	dle typu hosta a jeh	null	ne
ne	ne	ne	ne	ne	null	ne

teré z následujících prostředků jsou nasazeny na pracovních stanicích pro zajištění jejich bezpečnosti?					
Firewall třetích stran	Antivirus	Anti-Spyware	Anti-Spam	Anti-Malware	Jiné. Prosím uveďte produkty, které používáte:
ne	ne	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne
ne	ano	ne	ne	ano	ne
ano	ano	ano	ano	ano	ne
ne	ano	ne	ne	ne	ne
ne	ano	ano	ne	ano	ne
ne	ne	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne
ne	ano	ano	ne	ano	ne
ne	ano	ano	ano	ano	ne
ne	ano	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne
ne	ano	ne	ne	ne	ne
ne	ano	ano	ne	ano	ne
ne	ano	ne	ano	ne	ne
ne	ne	ne	ne	ne	ne

Jsou stanovena pro zaměstnance v souvislosti s instalací programového vybavení na pracovních stanicích pravidla?	Jsou stanovena pro studenty v souvislosti s instalací programového vybavení na pracovních stanicích pravidla?
null	null
Nejsou stanovena pravidla	Ano, platná pro všechny studenty
Ano, platná pro některé zaměstnance	Nejsou stanovena pravidla
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro některé zaměstnance	Nejsou stanovena pravidla
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Nejsou stanovena pravidla	Nejsou stanovena pravidla
null	null
Ano, platná pro některé zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro všechny zaměstnance	Nejsou stanovena pravidla
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro všechny zaměstnance	Ano, platná pro všechny studenty
Ano, platná pro některé zaměstnance	Ano, platná pro všechny studenty
null	null